Universidad Autónoma de Querétaro
Facultad de Informática
Maestría en Sistemas de Información: Gestión y tecnología

Opción de titulación
Tesis: Implementación de una suite de administración de accesos para el área de seguridad de la Información en el Banco Interamericano de Desarrollo

Que como parte de los requisitos para obtener el grado de
Maestría en Sistemas de Información: Gestión y Tecnología

Presenta:
Carlos Alejandro Campos Hernández

Dirigido por:
Dra. Sandra Luz Canchola Magdaleno

Dra. Sandra Luz Canchola Magdaleno Presidente	Firma
Dra. Rosa María Romero González Secretario	Firma
Dra. Ma. Teresa García Ramírez Vocal	Firma
M.S.I. Ana María Díaz Álvarez Suplente	Firma
Dra. Ana Marcela Herrera Navarro Suplente	Firma

M.I.S.D Juan Salvador Hernández Valerio
Director de la Facultad

Dra. Ma Guadalupe Flavia Loarca Piña
Director de Investigación y Posgrado

Centro Universitario
Querétaro, Qro.
Noviembre 2017

RESUMEN

Con la implementación de la herramienta CA Identity Suite es posible administrar la seguridad de las aplicaciones(Oracle, Unix, exchange, Active Directory, etc.) del Banco Interamericano de Desarrollo, de manera tal que cada usuario tenga los accesos de acuerdo a su rol y función en la empresa y así los datos estarán protegidos y asegurados en la organización

Se fundamenta y justifica la importancia que tiene el uso de una herramienta de administración de accesos dentro de una organización de alcance mundial. El tipo de investigación que se utilizará es de procesos administrativos. El sistema de provisionamiento y administración de accesos pretende gestionar 10,000 cuentas de usuarios.

Se administrarán los accesos a los sistemas de información de la organización de forma semiautomatizada y centralizada, mediante la suite de seguridad CA Identity Suite por parte del equipo de Seguridad de la Información. Esto permitirá comparar las ventajas de tener una herramienta que nos permita gestionar los accesos de todos los empleados a los diferentes sistemas de la organización en todos los ambientes.

Todos los resultados de los eventos de provisionamiento de cuentas y tareas realizadas por parte del área de seguridad de la información a través de la herramienta pueden ser auditados, reportados, graficados mediante un reporteador del mismo sistema, mediante la aplicación eTrust Audit de la misma suite o en los logs de las aplicaciones.

Palabras clave: Active Directory, Oracle, Unix, Provisioning, Exchange, correo, ERP, People Soft.

ABSTRACT

With the CA Identity Suite application implementation in the Inter American Development Bank´s Information Security area it is possible to manage the system applications(Oracle, Unix, exchange, Active Directory, etc) security by the Information security administrators. In such way every user must have access to the systems in accordance with his/her function and role in the organization, in this way the information will be protected and assured in the company.

In this investigation the implementation and use of one application that manages the user`s access inside the organization is based and justified in the importance that the system will provisioned and managed 10,000 users accounts in a world wide organization. This is an administrative process investigation.

The users access to the Bank`s systems will be granted in a semiautomated and centralized form through the CA Identity suite application by the Information Security Officers. This will allow to compare the advantages of having an application that manages the accesses of all the employees in the different systems and environments of the organization.

The provisioning process events executed by the Information security officers through the CA Identity Suite application can be audited, reported, charted by the application`s reporter through the eTrust Audit tool which belongs to the same CA Identity Suite or in the application´s logs.

Key words : Active Directory, Oracle, Unix, Provisioning, Exchange, correo, ERP, People Soft.

Para mis hijas

Karla Natalia

Sofia

3

AGRADECIMIENTOS

Mi Profundo agradecimiento a mi esposa, hijas, padres y hermanos. También me gustaría expresar mi inmensa gratitud y mi agredecimiento a mi directora de Tesis la Dra. Sandra Canchola con quien he tenido el gran lujo de trabajar.

Este trabajo de investigación no podría haber sido escrito sin la generosa ayuda de incontables individuos que han compartido conmigo sus conocimientos y competencia. Extiendo a todos ustedes mi profundo aprecio.

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

1.1 Justificación de la Investigación

Automatizar de forma rentable la creación y administración de cuentas de usuario y derechos de acceso al tiempo que garantiza el cumplimiento de políticas de seguridad.

Con este proyecto de investigación se pretende acelerar el aprovisionamiento de usuarios y la gestión de acceso de los usuarios a los recursos corporativos de acuerdo con las políticas del negocio. Aprovisionamiento con confianza. Proporcionar el contexto completo de las relaciones entre los usuarios, los derechos de acceso, recursos y actividades de los usuarios y las políticas de cumplimiento, para que pueda aprovisionar un usuario adecuadamente desde el principio.

Caracteristicas de este proyecto de investigación:

- Provisioning Workflow: Los flujos de trabajo de aprovisionamiento permiten autenticar usuarios para su facil creación, activación, desactivación o eliminación de las cuentas y los ID de usuario sin intervención manual. Totalmente automatizado el flujo de trabajo de aprovisionamiento puede ser iniciado por un evento desencadenante.
- Delegación del Provisioning Process: Delegación del espectro completo de los derechos de aprovisionamiento según lo determinado por la política de seguridad del Banco Interamericano de Desarrollo.
- Proceso de aprobación: funcionalidad solicitante / aprobador con la automatización ampliada, incluyendo varios pasos en serie / paralelo, el volumen y los flujos de trabajo de aprobación basados en políticas.
- Modelado de Usuario: Creación de una cuenta eligiendo uno o más usuarios "modelos" con una función de trabajo similar o requisitos de acceso similares.
- Generación de Alias user id: Calcula la creación del nuevo Alias ”User ID” de acuerdo a las reglas del negocio.
- Decubrimiento automático de Cuentas Huerfanas: Busca las cuentas creadas fuera del Provisioning process y las vincula a los usuarios a través de la exploración y correlación de identidad automático

16

1.2 Antecedente

La seguridad de la información inicio en los bancos, particularmente el banco de Citigroup fue pionero en integrar el área de seguridad de la Información en su organización después de que sufriera un ataque por parte de algunos hackers en la década de los 80´s.

Con la cultura de que en las organizaciones lo más importante es la información, las políticas de seguridad y las herramientas de administración deben ser seguras y confiables. La cadena de seguridad de la información de una empresa es tan fuerte como su eslabón más débil que en este caso son las personas, por lo cual la administración de los passwords y sus políticas deben ser muy fuertes, confiables y secretas.

Este trabajo de investigación está dirigido para empresas del ramo financiero y que tengan mas de 50 empleados o colaboradores

Los elementos más significativos de esta investigación son los usuarios(personas), el provisionamiento de sus cuentas de acceso de forma efectiva, las aplicaciones(Oracle, Unix, Windows, Exchange, Active Directory), los servidores y la aplicación CA Identity Manager y CA Provisioning Manager

Anteriormente, a finales de los años 90´s la administración de cuentas era de forma descentralizada, lo que quiero decir con esto es que cada aplicación se administraba de manera independiente, con este proyecto integraremos la administración de los accesos de todas las aplicaciones listadas en párrafo anterior de manera centralizada.

1.3 Importancia del tema.

La vida contemporánea tiene, como un elemento esencial, el uso de computadoras para lidiar con la información que se usa en las actividades empresariales, institucionales y personales. El cómputo es la tecnología de la información desde hace por lo menos tres décadas, y lo será en el futuro previsible.

Aunque se que la manipulación y uso adecuado y confiable de la información requiere que las propiedades de seguridad de la misma sean las adecuadas, es necesario que se difunda en nuestra sociedad una cultura de la seguridad de la información. Sólo si esto sucede, quienes hacemos uso de la información, que realmente somos todos, lo podríamos hacer con tranquilidad.

17

La preocupación por la seguridad de la información no data de la aparición de las computadoras a mediados del siglo pasado. Es una preocupación ancestral. Cada generación ha manejado la información con la tecnología que tenía disponible. En este momento la tecnología que se usa más es el cómputo. Y esta tecnología presenta características que la hacen extremadamente eficiente y altamente peligrosa.

1.4 Manejo de la información

En nuestra época se menciona con insistencia el término “tecnología de la información” como si fuera un fenómeno contemporáneo. Nada más lejos de la verdad. Siempre ha existido la tecnología de la información, o para ser mas preciso, el uso de la tecnología disponible para el manejo de la información. Más aún, las necesidades del manejo de la información han sido el motor de desarrollos tecnológicos y aun culturales importantes. En esta época la tecnología que se ha puesto a disposición de esta actividad es la computación, que además de cumplir esta función ha logrado transformar el concepto mismo de información y de su manejo. En este sentido, nuestra época es en efecto la época de la tecnología de la información.

Al referirnos a la informática estamos hablando acerca del manejo de información, lo cual abarca desde su computación, sistematización, creación, almacenamiento y transmisión. Estos procesos y requerimientos aparecen junto con nuestra especie, y hasta cierto punto la caracterizan. Son procesos muy anteriores a la aparición de cómputo. Sin embargo, desde la parte media de este siglo han sufrido una transformación radical debido al invento y uso generalizado de las computadoras. Y es solo en los últimos diez años que afectan potencialmente a nuestra vida diaria.[1]

OBJETIVOS

1.5 Objetivo General

Implementar un sistema adecuado para administrar las aplicaciones del Banco Inter Americano de Desarrollo con sede en Washington D. C. y de esta manera mantener la Integridad, Confidencialidad, Integridad, autenticidad y disponibilidad de la información.

Para este proyecto usaremos las siguientes herramientas de Administración de la empresa CA Technologies: la suite de eTrust, eTrust Access Control, eTrust Admin, eTrust Audit, eTrust Single Sign-on, CA Identity Minder, CA Provisioning Manager; para hacer el provisionamiento y administración de las cuentas de todos los empleados del banco en todos los ambientes.

1.6 Objetivos Particulares

I. Gestionar las diferentes aplicaciones(Active Directory, Oracle, Exchange y Unix) en múltiples ambientes del Banco Inter Americano de Desarrollo a través de la aplicación CA Identity Minder

II. Utilizar las capacidades de CA Identity Minder para el provisionamiento de las cuentas de los usuarios del banco con roles de provisionamiento, políticas, plantillas de cuentas y la relación entre roles, tareas y eventos.

III. Administrar más de 20 000 cuentas de empleados a nivel mundial y provisionar las cuentas de los usuarios en los sistemas y en los diferentes ambientes.

1.3 Historia del Banco InterAmericano de Desarrollo(BID)

La idea de una institución para el desarrollo de América Latina y el Caribe surgió por primera vez durante las actividades iniciales encaminadas a crear un sistema interamericano en ocasión de la Primera Conferencia Panamericana de 1890. Tuvieron que transcurrir casi siete decenios para que el BID se volviese una realidad bajo una iniciativa propuesta por el entonces Presidente de Brasil Juscelino Kubitschek. El Banco se fundó oficialmente en 1959, cuando la Organización de los Estados Americanos redactó el Convenio Constitutivo del Banco Interamericano de Desarrollo.

A lo largo de los años, el BID ha agregado nuevos países miembros y ha aumentado su capital nueve veces. Estas acciones han permitido que el BID incremente el apoyo al alivio de la pobreza y otros programas de desarrollo que han ayudado a transformar a América Latina y el Caribe. Si bien aún queda mucho por hacer, los indicadores sociales de la región mejoraron notablemente en varios aspectos, como alfabetización, nutrición y esperanza de vida.

REVISION DE LA LITERATURA

1.4 Antecedentes y justificación de la investigación

La seguridad de la información siempre ha existido en todo momento y a lo largo de la historia y ha sido manejada con la tecnología que se tenía en cada era. En nuestra época la tecnología que tenemos es el computo y los ordenadores. En los últimos años los bancos y en la milicia han incorporado la seguridad de la información en sus organizaciones.

19

Con la cultura de que en las organizaciones lo mas importante es la información, las políticas de seguridad y las herramientas de administración deben ser seguras y confiables. La cadena de seguridad de la información de una empresa es tan fuerte como su eslabón mas débil que en este caso son las personas, por lo cual la administración de los passwords y sus políticas deben ser muy fuertes, confiables y secretas.

Este trabajo de investigación esta dirigido hacia grandes organizaciones en particular del ramo financiero.

Los elementos mas significativos de esta investigación son los usuarios(personas), el provisionamiento de sus cuentas de acceso, aplicaciones, endpoints(Oracle, Unix, Windows, Exchange, Active Directory), servidores y la aplicación CA Identity Manager y CA Provisioning Manager.

Los usuarios no saben administrar las contraseñas de acceso, es necesario que los sistemas se sincronicen para crear reglas de seguridad fuertes.

1.5 JUSTIFICACIÓN

Consiste en la exposición de motivos o razones para su investigación.

Con el fin de administrar diferentes endpoints(Oracle, Unix, Windows, Exchange, Active Directory) en una sola aplicacion CA Provisioning Manager, aumentar la seguridad de la organizacion y de sus recursos'que voy a hacer', en una organizacion la informacion es lo mas importante. Con la centralizacion de la administracion de los diferentes endpoints se generan beneficios como reducir costos en la administracion de los sistemas. La aplicación(IDM) CA Identity Manager, CA Provisioning Manager y Access Control será administrada por area de seguridad de la informacion de la organización.

1.6 Problemática de la seguridad (Daltabuit 2007)

La segunda guerra Mundial fue un parteaguas histórico, en más de un sentido, especialmente para la seguridad informática. Las técnicas de ocultamiento no sólo se aplicaron al ámbito estrictamente militar sino también a las relaciones diplomáticas con los gobiernos, a la información sobre secretos comerciales e industriales, a la información científica y técnica y, sobre todo, a

mantener la información almacenada en las grandes computadoras que surgieron en esa época, oculta y a salvo de accesos no autorizados, entre otras aplicaciones.

La protección que la información guardada en las computadoras requería en ese entonces pudiera parecer sencilla a la luz de la época actual, ya que los equipos eran centralizados y las computadoras eran de propósito específico. Pero el hecho de que esas computadoras empezaran a ser multiusuario y multitarea, inició el camino sin retorno de las preocupaciones de seguridad informática y computacional actuales.

Después de la segunda Guerra Mundial, en la década de los 70 y 80´s cuando las computadoras se hicieron de propósito general y multiusuario, el panorama de la seguridad de la información empezó a cambiar de manera compleja. Ya las computadoras no procesaban información solamente militar, de estado, o científica. Se trataba ahora de proteger información tan diversa, dependiendo de las aplicaciones, que bien podían ser de tipo bancaria, nóminas, comercio de diferente naturaleza, etc.

La situación se tornó aún más compleja al surgir las microcomputadoras y con ello la necesidad de proteger información particular en distintos y numerosos ámbitos y lugares.

Con el surgimiento de las redes de computadoras, la situación se volvió patológica, ya que ahora había que proteger la información también durante su viaje por canales públicos y abiertos.

Actualmente el problema no termina aquí. Hoy, muchas de las actividades de la sociedad se realizan a través de redes de todo tipo. Estas actividades van desde comunicaciones y transferencia, proceso y acceso de información, hasta servicios bancarios, dinero y comercio electrónicos, entre otros. Igualmente se tienen tecnologías de código distribuible, que obligan a proteger no sólo la información sino también los recursos físicos y lógicos de las computadoras y redes contra usos ilícitos. De la misma forma se debe proteger la información y los recursos de cómputo contra programas malignos como son los virus, gusanos y otras calamidades lógicas que proliferan en las redes.

1.7 Primeros problemas de seguridad informática[1]

Historia del computo conceptos básicos

En 1946 se construye la ENIAC (Electronic Numerical Integrator and Computer). Totalmente

21

electrónica, de bulbos y digital. Se empezó en 1943 y se termina en 1946. Es construida por Mauchly y Eckert; pesaba 30 toneladas y contenía 18,000 bulbos. Es la primera computadora universal y podría realizar 100,000 operaciones por segundo.

Muy pronto aparecieron aplicaciones diversas, pero la mas importante fue el diseño de un sistema de defensa antimisiles (cuyo desarrollo fue provocado por la detonación en 1949 de la primera bomba atómica atómica de la Unión Soviética). El prototipo fue ampliado y en abril de 1951 se demostró la factibilidad de rastrear tres aviones de hélice que volaron por los cielos de Massachussets. Después de invertir millones de dólares y trabajar 10 años se termino SAGE (Semi-Automatic Ground Envirinment) un sistema de cobertura continental con 23 centros de operación, conectados a través de líneas telefónicas dedicada, (lo cual requirió que Bell Labs inventara el modem) conformado por dos computadoras interactivas redundantes que eran capaces de rastrear 400 aviones simultáneamente.

Cada centro de operaciones tenia mas de 50 empleados, o sea que estas computadoras interactivas eran compartidas por más de 1000 usuarios. Mediante nuevas técnicas de asignar a cada usuario los recursos disponibles cíclicamente (tiempo compartido).

Aprovechando su participación en este proyecto, IBM diseñó el famoso sistema SABRE (Semi-Automatic Business Related Environment) de reservaciones para American Airlines que se convirtió en el paradigma de los sistemas transaccionales en línea, que empezó a funcionar en 1964. Además aprovechó también la tecnología de almacenamioento de Whirlwind que estaba basada en núcleos magnéticos.

SAGE y SABRE dieron origen a la consola de operación estándar con un tubo de rayos catódicos, un teclado y un apuntador manual para seleccionar opciones que aparecían en la pantalla. O sea el entorno de cómputo personal que nos es familiar hoy.

1.8 Conceptos Basicos

1.8.1 Historia de Internet

La historia de Internet se remonta al temprano desarrollo de las redes de comunicación. La idea de una red de ordenadores diseñada para permitir la comunicación general entre usuarios de varias computadoras sea tanto desarrollos tecnológicos como la fusión de la infraestructura de la red ya existente y los sistemas de telecomunicaciones. La primera descripción documentada acerca de las

22

interacciones sociales que podrían ser propiciadas a través del networking (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider, del Massachusetts Institute of Technology, en Agosto de 1962, en los cuales Licklider discute sobre su concepto de Galactic Network (Red Galáctica).

Las más antiguas versiones de estas ideas aparecieron a finales de los años cincuenta. Implementaciones prácticas de estos conceptos empezaron a finales de los ochenta y a lo largo de los noventa. En la década de 1980, tecnologías que reconoceríamos como las bases de la moderna Internet, empezaron a expandirse por todo el mundo. En los noventa se introdujo la World Wide Web (WWW), que se hizo común.

1.9 Estado del Arte

A. Sistema de Provisioning IdentityIQ de sailpoint

Administración de Identidades y accesos

IdentityIQ es una solución de software de gestión de identidades y accesos(IAM) de la empresa Sailpoint que ofrece un enfoque unificado para el cumplimiento de políticas empresariales, administración de contraseñas y actividades de provisionamiento de cuentas en aplicaciones que se ejecutan en las instalaciones de los clientes o en la nube. IdentityQ satisface las necesidades de grandes organizaciones con procesos de gestión de identidades/usuarios complejas que prefieren adaptar su solución para alinearse con las necesidades comerciales especificas.

Sailpoint Technologies, (2017). *Identiry is Power* Recuperado el 14 de Febrero del 2017 de www.sailpoint.com

B. Sistema de Administración y Aprovisionamiento de Usuarios(COURION Provisioning)

Las soluciones de aprovisionamiento de Courion reducen la carga administrativa y los costos de administración de cuentas. facilitando el acceso abierto y compatible a través de múltiples plataformas y ambientes. Courion te ayuda a ser sensible a las necesidades de la empresa con el self-service y soluciones automatizadas de aprovisionamiento.

Recibir notificaciones automáticas de acceso inadecuado o violaciónes de política en el punto de provisioning.

23

Core Security, (2016). *The Access Assurance Suite* Recuperado el 14 de Febrero del 2017 de **http://www.courion.com/solutions/provisioning**

C. Sistema de Administración y Aprovisionamiento de Usuarios (CURA3)

Es una solución para autenticar, autorizar y administrar de manera centralizada identidades, control de acceso y aprovisionamiento de usuarios. Un servidor centralizado de autenticación que utiliza métodos fuertes como son: Password dinámico (Tokens), certificados digitales X.509 v3, Tokens USB, Biometría.

Permite la Integración simple de aplicaciones mediante APIs y la sincronización de contraseñas, privilegios y características del usuario en plataformas remotas, por ejemplo, sistemas operativos, bases de datos, aplicaciones “legacy”.

Además se caracteriza por ser una solución completa de PKI y autoridad certificadora.

Características:

- Administración centralizada de usuarios y recursos.

- Administración de identidades y accesos (Password Único)

- Administración de reglas de control de accesos

- Control y administración del ciclo de vida de un usuario en la empresa y su asignación de recursos.

- High availability scheme.

- Sistema para el enrolamiento de usuarios integrado con sistemas AFIS

- Fácil Integración con métodos biométricos.

- Manejo de reglas de contraseñas

- Esqueletos de ARAs para aplicaciones y sistemas no soportados out-of-the-box.

- Subsistemas de bitácoras, auditoría y revisión.

- Sistema de alertas y alarmas de acuerdo a las reglas de negocio establecidas por la organización.

- Capacidad de tolerancia a fallas y balanceo de cargas para todos los procesos.

- Solución de Public Key Infrastructura (PKI) y autoridad certificadora.

Sistema de Administración y Aprovisionamiento de Usuarios (CURA3)

CURA3 Access

Es una solución completa de control de accesos que provee las funcionalidades necesarias para una administración eficaz en las operaciones de seguridad de una empresa.

- Permite tener un control y registro exacto de entradas y salidas de empleados, proveedores y visitantes, así como las áreas que fueron accedidas mediante tarjetas de proximidad.

- Con la información obtenida se pueden generar reportes históricos de todas las alarmas o eventos en los accesos protegidos por la solución dentro de la organización.

- Monitoreo de todos los eventos que ocurran en tiempo real

- CURA3 Access posee una interfaz gráfica de administración basada en roles y permisos, con la posibilidad de manejar desde usuarios individuales con múltiples responsabilidades hasta aquellos que realizan funciones sencillas y poder restringir el acceso a áreas específicas

- Su arquitectura permite una rápida y fácil instalación, sin la necesidad de requerir de recursos adicionales de hardware o software.

Sistema de Administración y Aprovisionamiento de Usuarios (CURA3) (2015). INSYS-CORP Recuperado el 14 de Febrero del 2017 de **http://www.insys-corp.com.mx**

25

METODOLOGIA

General

1.10 Descripcion del proyecto

Implementacion del sistema Enterprise Identity and Access Management(EIAM), Identity Manager(IDM) y Provisioning Manager(PM)

Mejorar la eficiencia y efectividad de los procesos de acceso, aprovisionamiento en el Banco Interamericano de desarrollo(IDB) con un enfoque empresarial más sólido y global.

Para obtener los beneficios de una solución empresarial como Enterprise Identity and Access Management(EIAM), Identity Manager(IDM) y Provisioning Manager, en este proyecto se esboza un enfoque de tres fases

- Fase 1: construir los cimientos de la aplicación EIAM y concentrarse en sistemas críticos

  - Las áreas de enfoque: Administrar y gestionar identidades, matriculación, solicitudes de acceso, flujo de trabajo, aprovisionamiento, administración de aplicaciones y de usuarios mediante a roles, administración de contraseñas(Self Service), evaluación de riesgos, auditoria y revisión periódica de accesos.

- Fase 2: Aumentar las capacidades de la aplicación EIAM para administrar sistemas críticos

  - Las áreas de enfoque: Capacidad de autentificación y gestión de acceso centralizado, capacidad de control de acceso en base a un role, reglas en base en asignación de roles, implementación de reglas de auditoria empresarial, reglas de separación de deberes y administración centralizada del riesgo

- Fase 3: extender las capacidades de IDM creadas en previas fases para heredar aplicaciones y nuevas iniciativas tales como ejecutar riesgo en base en análisis.

26

- Las áreas de enfoque: autorización centralizada y administración de autorización, riesgo basado en autenticación, riesgo basado en reforzamiento de políticas y riesgo basado en monitoreo de usuarios privilegiados con muchos accesos y accesos críticos.

1.11 Alcance

Funcionalidad incluye:

- Instalación de Identity Manager en los tres ambientes(Desarrollo, Pruebas y Producción)
- Directorio Activo (Active Directory) – dos dominios
- Cliente de correo electrónico Exchange365
- Integracion de People Soft(Recursos Humanos) fuente autorizada del provisioning process
- Administracion de contraseña - Cuentas de Usuario de Unix y Oracle
- Auditoria y reportes
- Administración, adquisición de 30 bases de datos de Oracle
- Administracion de 22 servidores de Unix AIX via el conector CA Control Minder
- Creacion de tickets automáticos en la herramienta de control de incidentes y problemas(Service Now) accionados por las notificaciones de email que genera la herramienta EIAM Provisioning Manager

27

1.12 Requerimientos del sistema

1.12.1 Requerimientos específicos de Aplicación

People Soft (ver Tabla 1)

Proposito: Provisionar de accesos a los nuevos ingresos del banco que necesiten acceso a los sistemas, suspender todos los accesos de los usuarios que han terminado contrato con el banco y que tienen acceso a los sistemas, Transferir usuarios de una Unidad organizacional a otro, Hacer la reactivación de accesos de los usuarios que han sido recontratados en el banco y necesitan acceso a los sistemas.

Capturar todos los datos disponibles en Recursos Humanos de los usuarios que serán usados para correlacionar identidades entre IAM y todos los otros en point systems(Oracle, Active Directory, Unix, Exchange)

Supuestos:

- Una unidad de un servidor Windows es compartido en la red [dataprot(pruebas), dataprop(producción)] ha sido configurado para que reciba el archivo de texto txt llamado Prov_file con todos los records de los empleados(activos e inactivos) que exiten o existieron en el banco. El archivo de texto(Prov_file) proviene de peoople Soft. Esta es la fuente para procesar el psfeed(Provisioning)

- Todos los records de empleados activos y terminados del banco IDB se encuentran en People Soft

- Todos los datos requeridos para la creación de cuentas de Active Directory se obtendrán de los records del archivo txt llamado prov_file.

- Todos los records aparecen en le archivo de texto Prov_file la primera vez que tienen el status de activo (Status = 1)

- Los usuarios que tienen acceso a los sistemas son los que tiene banderas de provisioning de YY en sus records

- **Tabla 1 - People Soft**

NO REQ	REQUERIMIENTO FUNCIONAL
PSFT-1.	People Soft enviará un archivo txt todos los días por la mañana(6:30am) con todos los records de los usuario que tienen o han tenido contrato en el Banco. Este archivo es la fuente de datos autoritativa de Recursos Humanos.
PSFT-1.1	El Sistema de People Soft agregara un archivo txt con los records de los contratos del Banco todos los días por la mañana a las 6:30 am en un drive compartido de un servidor de Windows
PSFT-1.3	El sistema correlacionara los datos del empleado provenientes de People Soft para las identidades existentes en el sistema basado en el EmployeeID, el cual es el único dato para indexar
PSFT-1.4	El sistema permitirá buscar identidades por ambos employeeID y Aliasname.
PSFT-1.5	Cuando un dato de alguna identidad es actualizado en People Soft, el sistema IAM actualizará todos los atributos de esa Identidad en los endpoints asociados
PSFT-1.6	El sistema creará una entrada de auditoría cuando un record de un empleado es invalido en el archivo de datos txt, archivo de texto Prov_file

Esquema de PeopleSoft(ver tabla 2)

Este es el esquema de un record de usuario

UserName|FullName|FirstName|LastName|MiddleName|employeeID|EnableDt|DisableDt|DeptId|Title |Company|Phone|PrimaryMail|ManagerId|ManagerUserName|Status|PreferredFirstName|Location|D eptDescr|EmpldRcd|StreetAddress|City|State|PostalCode|Country|UserType |ADAccount|EmailAccount|AlternateEmplid

Tabla 2 - A continuación se describen cada uno de los campos del record de un usuario

Nombre del campo	Tipo de dato	Valores Validos	Descripciom/Notas	Identidad Atributo?	Valor Unico?	Nulos permitidos?
Nombre de Usuario	Texto		Alias de la identidad	Si	Si	Si
Nombre Completo	Texto		Nombre completo de la identidad	Si	No	No

29

Nombre del campo	Tipo de dato	Valores Validos	Descripciom/Notas	Identidad Atributo?	Valor Unico?	Nulos permitidos?
Nombre	Texto		Legal primer nombre de la identidad	Si	No	No
Apellido	Texto		Legal apellido de la identidad	Si	No	No
Segundo Nombre	Texto		Legal Segundo nombre de la identidad	Si	No	Si
ID de empleado	Número	6 digitos número	Número de empleado, identificador único de la identidad	Si	Si	No
Fecha de habilitación	Date	MM/DD/YYYY	Fecha de habilitación para el status de la identidad	No	No	No
Fecha de deshabilitación	Date	MM/DD/YYYY	Fecha de deshabilitación para el status de la identidad	No	No	Si
ID de departamento (DeptId)	Texto		Departamento de la identidad de forma abreviada(DeptId)	Si	No	No
Titulo	Texto		Titulo de la identidad	No	No	Si
Compañia	Texto	IDB / IIC	Compañía de la identidad	Si	No	No
Teléfono	Texto	XXX/XXX-XXXX	Número de teléfono de la identidad	Si	No	Si
Email primario	Texto		e-mail primario de la identidad	Si	No	Si
Manager Id	Número	6 digitos número	Identificador único del manager de la identidad	Si	No	Si
Nombre de usuario del manager del usuario	Texto		Alias del manager de la identidad	Si	No	Si
Status	Boolean	0,1	Status de la identidad 0 = inactivo, 1 = activo	Si	No	No
Ubicación	Texto	HQ o abreviación del pais	Ubicación de lugar de trabajo de la identidad	Si	No	No
Descripción del departamento(DeptDescr)	Texto	Org / Unit	Descripción del departamento de la identidad	Si	No	No
Numero de contrato (EmpldRcd)	Número		Número de contrato de los consultores, para los Staff es null	No	No	Si
Dirección(calle)	Texto		Dirección de la Organización	No	No	Si
Ciudad	Texto		Dirección de la Organización	No	No	Si
Estado	Texto		Dirección de la Organización	No	No	Si
Codigo Postal	Texto		Dirección de la Organización	No	No	Si
Pais	Texto		Dirección de la Organización	No	No	Si
Tipo de usuario	Texto	Staff Contractor Contractual		Si	No	No
Cuanta de Active Directory	Boolean	Sí, No	Bandera de estado si el AD necesita ser provisionado	Si	No	No
Cuanta de e-mail	Boolean	Si, No	Bandera de estado si excahnge necesita ser provisionado	Si	No	No
Número de empleado alterno	Número	6 digitos número	Ultimo número de empleado de la identidad	Si	Si	Si

Ejemplo de un record de usuario:

SOLVEIR|Rasmussen,Solvei|Solvei|Rasmussen||777500|03/01/2016|03/01/2020|ITE/ITE|Smoke Test User|IDB|202/623-1277|| ||1| |HQ|InterAmerican Development Bank| 1| | | | |Staff|Y|Y|

Todos los records de los usuarios se encuentran en el archivo de texto Prov_file

Active Directory(ver tabla 3)

Propósito: Para provisionar datos del dominio de Active Directory con el propósito de crear nuevas cuentas o actualizar membresías de grupo. Aditionalmente, habrá un proceso para agregar y reconciliar cuentas periodicamente

Supuestos: El sistema será configurado para conectar tres dominios de IDB: IDB, IIC, REG

Tabla 3 – Active Directory

NO REQ	REQUERIMIENTO FUNCIONAL
AD-1. Reconciliar datos del dominio de Active Directory y permitir el provisionamiento de cuentas.	
AD-1.1	El sistema será configurado para conectar el dominio en Active Directory en dos ambientes: Pruebas y Producción.
AD-1.2	El sistema tendrá acceso de lectura y escritura de datos a través de una cuenta de servicio única en ambos ambientes
AD-1.3	El sistema agregara datos de cuenta y grupos del dominio de Active Directory de acuerdo a las bases del día a día
AD-1.4	El sistema permitirá a todos los usuarios activos autenticarse al sistema usando sus usuarios y contraseñas de Active Directoy
AD-1.5	El sistema mandará una notificación de correo electrónico para el grupo de trabajo de Security cuando exista un evento en el sistema como una Terminación, una transferencia, un usuario nuevo(nueva contratación) o una recontratación(reactivación)
AD-1.6	El atributo clave o primario que se correlaciona entre el sistema y el Active Directory para cuentas de usuarios es el número de empleado, la correlación es de “Employee ID” a “employeeID”
AD-1.7	El sistema correlacionara cuentas de administrador en Active Directory en las siguientes OU y sus sub OUs(SAP, TCS, Tmp, Disabled …etc)
AD-1.8	El sistema permitirá a los administradores correlacionar las cuentas manualmente

AD-1.9	El sistema permitirá a los administradores de seguridad de la información habilitar o deshabilitar una cuenta de Active Directory manualmente

Active Directory(ver tabla 4)

Proposito: crear una cuenta de active directory para un usuario nuevo y poblar apropiadamente los atributos de AD y los permisos de grupo. Esta cuenta será poblada con más información del usuario durante el proceso HR2AD después de la creación.

Supuestos: Asignacion de la unidad organizacional OU será basado en el mapeo proveniente del archivo de texto .txt(Prov_file) de Recursos Humanos

Tabla 4 – Active Directory

NO REQ	REQUERIMIENTO FUNCIONAL
AD-2. Crear una cuenta de Active Directory con los atributos correctos y con los grupos y permisos apropiados.	
AD-2.2	El sistema usará la siguiente lógica para asignar una Org Unit para una identidad usando el mapa de la tabla de Org Units: Si las últimas tres letras en “Department ID” es un código de un país, entonces asignar la cuenta al dominio REG (REG/COF) usando la tabla del mapeo de los paises Si el código del país no se encuentra en la tabla entonces el sistema mandará un error y se hará el trabajo manualmente
AD-2.3	El sistema generará una tarea manual para el equipo de provisioning si una unidad orgaizacional válida no es encontrada.
AD-2.4	El sistema asignará la nueva cuenta a un grupo de Active Directory basado en el nombre de la OU.

32

AD-2.5	El sistema asignará los siguientes grupos de Active Directory a las identidades con “UserType” = “Staff” en la OU “EXD” (exepto identidades con “DeptID” = “EXD/099”): EXD EXD_Portal Zenprise MDM EXD Users BI_EDW_EXD_CONSUMERS EXD-XXX (example: Dept ID: “EXD/001” -> AD Group “EXD-001”) EXD-XXX-YY (example2: Dept ID: EXD/002 -> AD Groups: EXD/002-CH, EXD/002-EC …etc)
AD-2.6	El sistema asignará el siguiente grupo de Active Directory a las identidades con “UserType” = “Staff” y “DeptID” = “EXD-099”: EXD

Los siguientes atributos son requeridos para la creación de AD. (ver tabla 5)

Tabla 5 - Esquema de Active Directory

Atributo de Active Directory	Atributo de la identidad
Cn*	Upper case(<alias>)
distinguishedName*	CN=< Upper case(<alias>)>,OU=Users,OU=<first three letters of Department ID>,OU=<location>,DC=<domain>**,DC=iadb,DC=org
employeeID	EmployeeID
givenName	First Name
Initials	Middle Initial
displayName	Full Name
sAMAccountName	Lowercase(<alias>)
userPrincipleName	<alias>@iadb.org
Sn	Last name
extensionattribute1	UserType
Department	DeptID
Manager	ManagerId|ManagerUserName

** Domain= If the last three letters in “Department ID” is a country code => Domain=**REG** if not Domian=**IDB** .

1.12.1.1 Mapa de los países del dominio REG en Active Directory

La siguiente tabla contiene los códigos de los países y sus correspondientes OU in el dominio REG de Active Directory(ver tabla 6)

Tabla 6 - Mapeo de los países

Código de país	Nombre de País	OU en REG
CCO	Colombia	CCO
EUR	Europa	CFR
CAR	Argentina	CAR
CCR	Costa Rica	CCR
CVE	Venezuela	CVE
CBH	Bahamas	CBH
CBL	Belize	CBL
CBO	Bolivia	CBO
CBR	Brasil	CBR
CCH	Chile	CCH
CEC	Ecuador	CEC
CES	El Salvador	CES
CGU	Guatemala	CGU
CGY	Guyana	CGY
CHO	Honduras	CHO
CJA	Jamaica	CJA
CNI	Nicaragua	CNI
CPE	Perú	CPE
CPN	Panamá	CPN
CPR	Paraguay	CPR
CTT	Trinidad y Tobago	CTT
CUR	Uruguay	CUR
CME	México	CME
CSU	Suriname	CSU
CHA	Haití	CHA
CDR	República Dominicana	CDR
CBA	Barbados	CBA
ASI	Japon	CJP
INL	INTAL	INTAL

Exchange – Correo electrónico(ver tabla 7)

Proposito: Agreagar datos de Exchange y correlacionar las identidades existentes. El sistema estará disponible para provisionar y deprovisionar las licencias de Exchange de los usuarios basado en el workflow del ciclo de vida de los contratos de los usuarios.

Supuestos: Los nombres de cuentas de Exchange simpre coincidirán con el alias de la identidad debido a la sincronización con Active Directory.

El sistema será responsable del provisionamiento de licencias de Exchange a las cuentas de las identidades y también será responsable de la creación de buzones de correo electrónico.

34

Tabla 7 – Exchange

NO REQ	REQUERIMIENTO FUNCIONAL
EX-1. Agregar datos de cuenta de usuario y permitir el provisioning y deprovisioning de las licencias de exchange.	
EX-1.1	El sistema adquirirá acceso de lectura y escritura en los datos de la cuenta del usuario, usando una cuenta de servicio única.
EX-1.2	El atributo de correlacion entre Exchange y la cuenta de active directory del usuaro es el “Alias”/UserName
EX-1.3	El sistema agregará datos de licencia de Exchange de acuerdo a las bases diarias de provisioning
EX-1.4	El sistema permitirá a los administradores correlacionar las cuentas manualmente.
EX-1.5	El sistema estará disponible para provisionar y deprovisionar licencias de Exchange.

UNIX(ver Tabla 8)

Proposito: Agregar datos de servidores de Unix y correlacionar cuentas y grupos para identidades existentes. El sistema será capaz de deprovisionar cuentas de UNIX basado en el ciclo de vida del contrato del usuario.

Supuestos: El sistema provisionará y deprovisionará cuentas de unix

Tabla 8 - UNIX

NO REQ	REQUERIMIENTO FUNCIONAL
UNX-1. Agregar y reactivar cuentas de Unix y permitir el deprovisionamiento de cuentas de Unix. Agregar datos a las cuentas de Unix y obtener datos de servidores Unix.	
UNX-1.1	El sistema se configurará para conectarse a los servidores de UNIX usando un conector el cual interactuará con CA Control Minder.
UNX-1.2	El sistema obtendrá acceso de lectura y escritura en los datos de la cuenta de usuario usando una cuenta de servicio único.

35

NO REQ	REQUERIMIENTO FUNCIONAL
UNX-1.3	El atributo de correlación entre UNIX y el sistema será UserName/Alias si el alias de la identidad es menor o igual a 8 caracteres.
UNX-1.4	El atributo de correlación entre UNUIX y el sistema será el nombre completo si el alias de la identidad es mayor a 8 caracteres.
UNX-1.5	El sistema será capaz de aceptar un texto plano de todas las cuentas existentes de UNIX para la correlación inicial de la carga del sistema
UNX-1.6	El sistema provisionará cuentas y datos a los 30 servidores UNIX de desarrollo, pruebas y producción.
UNX-1.7	El sistema generará un reporte de cuentas no correlacionadas.
UNX-1.8	El sistema permitirá a los administradores correlacionar las cuentas manualmente.
UNX-1.9	El sistema permitirá a los administradores habilitar y deshabilitar las cuentas de UNIX manualmente.
UNX-1.10	El sistema deprovisionara las cuentas de UNIX suspendiendo la cuenta del usuario y removiendo los grupos asociados dejándolos de la siguiente manera(set home Empty, Login Bin/false, set primary group Usr, remover grupos nativos de UNIX y de etrust) via un conector de Control Minder.

Oracle(ver Tabla 9)

Proposito: Agregar datos de Bases de datos de Oracle y correlacionar cuentas para identidades existentes. El sistema será capaz de deprovisionar cuentas de Oracle basado en el ciclo de vida del contrato del usuario.

Supuestos:

- El sistema deprovisionará cuentas de Oracle.
- El sistema conectará con bases de datos de desarrollo, pruebas y producción

36

El sistema recuperará Oracle username, profile, role(default, con opciones de admin) y privilegios de sistema (Tablespace: Default y temporary, Account Status, expire password) durante la agregación

Tabla 9 - Oracle

NO REQ	REQUERIMIENTO FUNCIONAL
ORA-1. Agregar y reactivar cuentas de Oracle y permitir el deprovisionamiento de cuentas de Oracle. Agregar datos a las cuentas de Oracle y obtener datos de servidores y base de datos de Oracle.	
ORA-1.1	El sistema será configurado para conectarse a las bases de datos de Oracle con cuentas de servicios(svc_fie_tst, svc_huris_prd, SVC_LMS_TST, etc)
ORA-1.2	El sistema obtendrá acceso de lectura y escritura en los datos de la cuenta de usuario usando una cuenta de servicio único.
ORA-1.3	El atrubuto que correlacionará el nombre de usuario de Oracle y el userID de la identidad/usuario es el “Alias”.
ORA-1.4	El atributo que correlacionará entre la cuenta de Oracle DBA y el sistema será basado en el alias del usuario pero tendrá el prefijo de “OPS$”. Ej. (cuenta de Oracle “OPS$JohnS” será correlacionada con el usuario “JohnS” en el sistema).
ORA-1.5	El sistema agregará datos de cuenta de las bases de datos de Oracle de desarrollo, pruebas y producción de acuardo a las bases diarias del sistema EIAM
ORA-1.6	El sistema permitirá a los administradores correlacionar manualmente las cuentas.
ORA-1.7	El sistema permitirá a los administradores habilitar y deshabilitar las cuentas de Oracle manualmente.
ORA-1.8	El sistema estará disponible para deshabilitar y deprovisionar(remover todos los permisos) las cuentas de Oracle.

Cambio de alias Manual(ver Tabla 10)

EL cambio de Alias manual provee a los miembros del equipo de provisioning con el poder de cambiar el alias/userId de un usuario/identidad manualmente. El administrador debe revisar que el

37

alias solicitado este disponible, si está disponible entonces se aplica manualmente el renombre del alias en active directoy.

Proposito: Permitir a los administradores cambiar el alias de una identidad/usuario manualmente

Supuestos:

- El sistema estará disponible para renombrar las cuentas de Active Directory
- El sistema no renombrará cuentas de Oracle
- El sistema no renombrará cuentas de Unix

El sistema re-asociará todas las cuentas (Oracle, Unix) con el nuevo Alias

Tabla 10 - Cambio de alias Manual

NO REQ	REQUERIMIENTO FUNCIONAL
MAC-1. Cambio de alias manual de una identidad/usuario	
MAC-1.1	El sistema tendrá una opción llamada renombrar Alias que es accesible para los administradores
MAC-1.2	La opción de cambio de alias manual mostrará las cuentas asociadas con el usuario seleccionado: Active Directory, Exchange, Oracle y Unix.
MAC-1.3	El sistema permitirá a loas administradores checar la disponibilidad de un Alias.
MAC-1.4	El sistema permitirá a los administradores cambiar el alias de la identidad/usuario y propagarlo a la cuenta del directorio activo
MAC-1.5	El sistema correlacionará cualquier cuenta de Oracle con el nuevo Alias sin cambiar el username de las cuentas de Oracle.
MAC-1.6	El sistema correlacionara cualquier cuenta de Unix con el nuevo Alias sin cambiar el username de las cuentas de Unix

38

Suspension de cuenta manual(ver Tabla 11)

Proposito: permitir a los administradores suspender una cuenta de usuario inmediatamente de forma manual a traves del sistema, esta acción deshabilitará las cuentas que el uausrio tenga conectadas dentro de su usuario global

Supuestos: Esta función hará los mismos pasos que el flujo de trabajo de Terminación/off-boarding

Tabla 11 - Suspensión de cuenta manual

NO REQ	REQUERIMIENTO FUNCIONAL
IMTRM-1. Terminacion de cuenta de usuario manual	
IMTRM-1.1	El sistema tiene una opción para terminar/suspender de manera manual a un usuario, y esta opción es accesible para los administradores.
IMTRM-1.2	El sistema permitirá a los administradores activar el proceso y flujo de trabajo de una terminación/off-boarding de un usuario basado en las bases diarias del provisioning
IMTRM-1.3	El sistema mostrará el log/bitácora el nombre de la persona que procesó la acción de termination/off-boarding manual.

REQUERIMIENTOS DE CICLO DE VIDA DE UNA IDENTIDAD

Requerimientos funcionales de un proceso de ciclo de vida de una cuenta de usuario

La sección detalla los requerimientos de una identidad en el todo el proceso de ciclo de vida

39

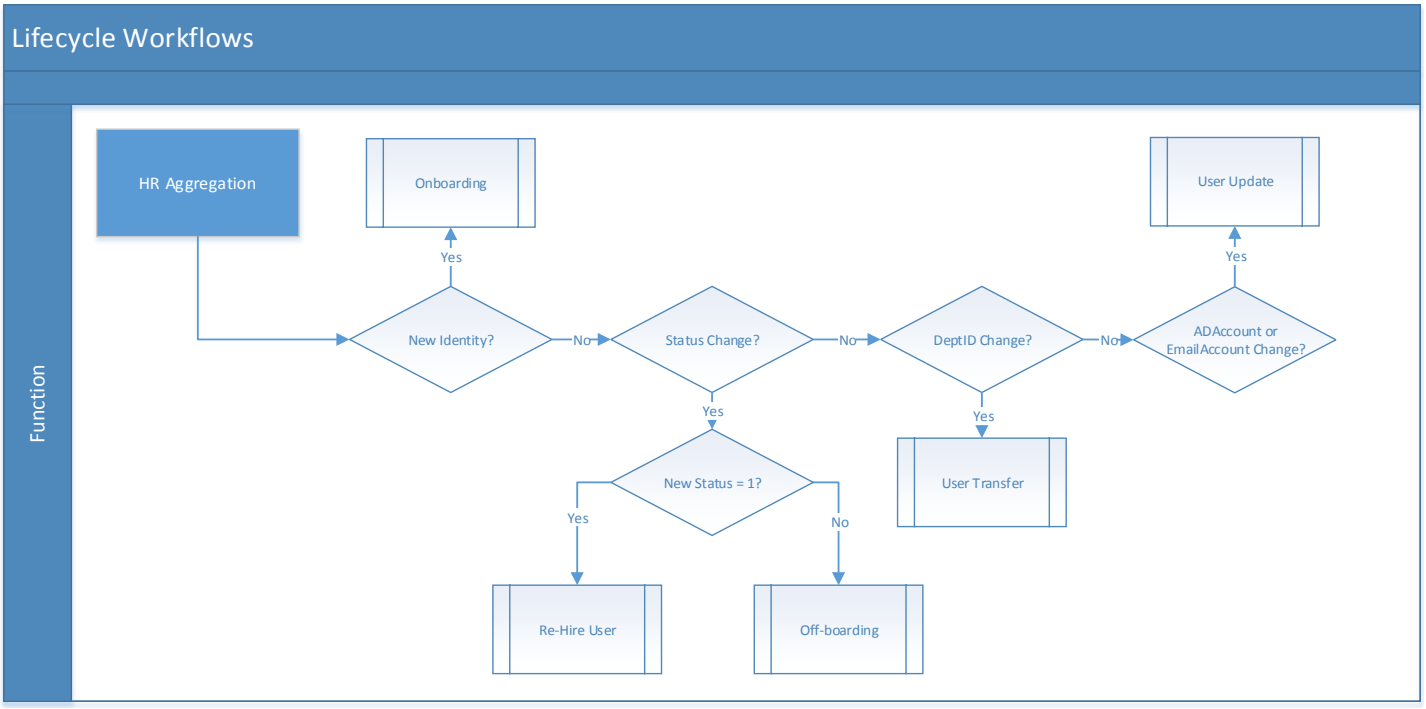


Figura 1: flujo de trabajo de ciclo de vida

Requerimientos de Ciclo de vida(ver Tabla 12)

Proposito: Inicializar propiamente los eventos del ciclo de vida basados en el cambio de los datos/información del sistema fuente(prov_file). Los eventos del ciclo de vida de una cuenta de usuario será manejado por el provisionamiento y deprovisionamiento de todas las plataformas conectadas.

Supuestos: El sistema fuente(Prov_file) de PeopleSoft desencadenará los eventos de ciclo de vida basados en los cambios de esta aplicación.

Tabla 12 - Requerimientos de Ciclo de vida

NO REQ	REQUERIMIENTO FUNCIONAL
LFCYC-1.	**El sistema monitoreará los cambios en los atributos de las identidades/usuarios y desencadenará los eventos de ciclo de vida basado en condiciones predefinidas.**
LFCYC-1.1	El sistema iniciará el proceso de “new user” para cualquier record del sistema fuente(Prov_file) de PeopleSoft cuando el “Status” sea “1”.
LFCYC-1.2	El sistema iniciará el proceso de “Terminación” para cualquier record del sistema fuente(Prov_file) de PeopleSoft cuando el “Status” cambie de “1” a “0”.

NO REQ	REQUERIMIENTO FUNCIONAL
LFCYC-1.	**El sistema monitoreará los cambios en los atributos de las identidades/usuarios y desencadenará los eventos de ciclo de vida basado en condiciones predefinidas.**
LFCYC-1.3	El sistema y los administradores identificarán usuarios con multiples números de empleado con el atributo número de empleado alterno(“AlternateEmplid”)
LFCYC-1.4	El sistema iniciará el proceso de reactivación(Recontratación) para cualquier record existente en el sistema fuente(Prov_file) de PeopleSoft cuando el “Status” cambie de “0” a “1”.
LFCYC-1.5	El sistema iniciará el proceso de una “Transferencia” para cualquier record existente en el sistema fuente(Prov_file) de PeopleSoft cuando su departamento cambie de un departamento a otro, atributo ”Department ID”
LFCYC-1.6	El sistema iniciará una “actualización de usuario” para cualquier record existente en el sistema fuente(Prov_file) de PeopleSoft cuando cambie su ManagerID o su fecha de termino de contrato

Flujo de trabajo de un nuevo usuario/Onboarding

Esta sección describe los pasos del proceso de un nuevo usuario/Onboarding que el sistema tomará para crear una identidad/usuario del banco IDB usando datos del sistema de People Soft.

El flujo de trabajo de un nuevo usuario iniciará cuando el sistema fuente de Recursos humanos People Soft dispare el inicio del contrato del usuario o cuando las banderas de provisioning del usuario cambien de NN a YY. El sistema de provisioning manejará todas las cuentas requeridas y mandará una notificación de creación de un usuario nuevo a diferentes áreas

41

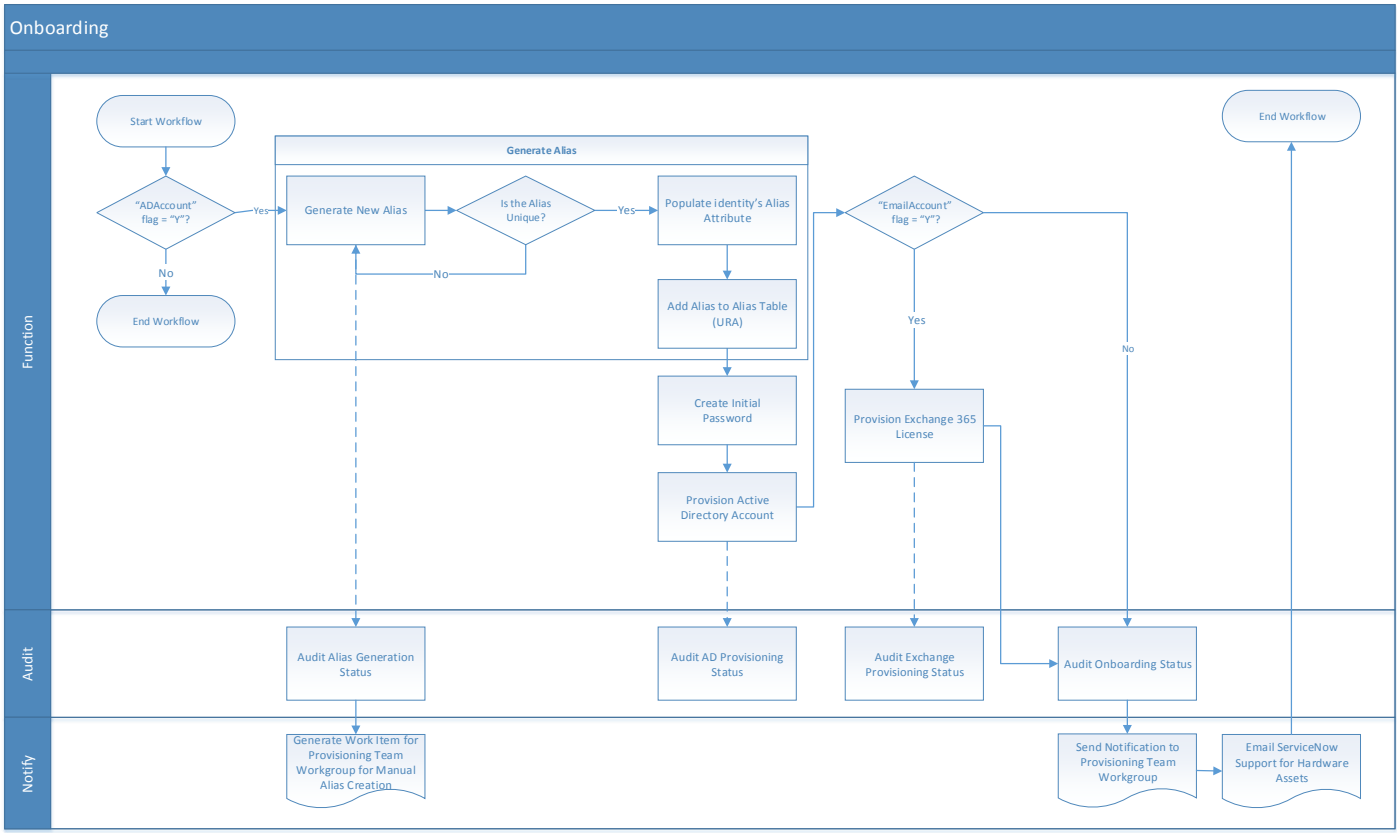


Figura 2: Flujo de Trabajo de Nuevo usuario/Onboarding

Requerimientos de Nuevo Usuario/Onboarding(ver tabla 13)

Proposito: Asignar un alias único para todos los usuarios nuevos con contratos validos y con banderas de provisioning YY o YN en Active Directory basado en una metodología lógica predefinida.

El flujo de trabajo del proceso de un usuario nuevo inicia después de que el contrato del usuario es ingresado en People Soft, posteriormente el proceso de provisioning manejará la creación de todas las cuentas solicitadas.

- Active Directory
- Exchange

Supuestos: IDB proveerá una lista maestra de todos los aliases actuales que serán guardados en el sistema para prevenir creaciones de alias duplicados.

42

Tabla 13 - Requerimientos de Ciclo de vida

43

NO REQ	REQUERIMIENTO FUNCIONAL
ONBRD-1.	**El sistema generará un alias único para los nuevos usuarios**
ONBRD-1.1	El sistema creará un “Alias” para la identidad/usuario solo si el atributo “AD Account Flag” se establece como “Y”.
ONBRD-1.2	El sistema checará la unicidad de la generación de los aliases checando que el alias no exista en el archivo existing user y en el portal de URA(el cual guarda todos los usersIDs históricos).
ONBRD-1.3	El sistema creará el “Aias” usando solo caráctares alpha(solo letras).
ONBRD-1.4	El sistema reemplazará los siguientes carácteres durante la creación del “Alias”. • “á" con "a" • “é" con "e" • “í" con "i" • “ó" con "o" • “ú" con "u" • “ñ" con "n"
ONBRD-1.5	El sistema automaticamente generará un alias basado en la siguiente combinación de atributos en prioridad de orden, asignando un único resultado para la identidad/usuario: Ejemplo: Nombre completo= Peter Bunny Rabbit 1. PrimerNombreInicialApellido (PETERR) 2. InicialPrimerNombreApellido (PRABBIT) 3. InicialPrimerNombreInicialSegundoNombreApellido(PBRABBIT) 4. PrimerNombreInicialApellido (2) (PETERRA) 5. PrimerNombreInicialApellido (3) (PETERRAB) 6. InicialPrimerNombreSegundonombreInicialApellido (PBUNNYR) 7. Primernombre(3)InicialsegundonombreApellido (PETBRABBIT) 8. InicialPrimerNombreSegundonombreInicialApellido (2) (PBUNNYRA) 9. InicialPrimerNombreSegundonombreInicialApellido (3) (PBUNNYRAB) 10. Excepción

44

	El sistema se asegurará de que el “Alias” de una identidad/usuario sea mayor o igual a 4 caracteres.
ONBRD-1.6	El sistema limitará la creación del “Alias” de una identidad/usuario a 11 caracteres.
ONBRD-1.7	Los administradores crearan el alias de la identidad/usuario manualmente si el alias único no puede ser generado por el sistema basado en la metodología descrita en ONBRD-1.5 arriba.
ONBRD-1.8	El sistema permitirá a los administradores de Provisioning cambiar el Alias de una identidad/usuario manualmente si el que se creó está fuera de la política con la metodología descrita en ONBRD-1.5 arriba.
ONBRD-1.9	El sistema agregará el nuevo alias a la tabla de Aliases historicos.
ONBRD-1.10	El sistema creará un password inicial complejo con la generación del alias basado en los requerimientos de password especificados en la sección de password Management(administración de password)
ONBRD-1.11	El sistema creará una cuenta de Active Directory para usuarios nuevos basado en la sección de atributos, esquema de active Directory
ONBRD-1.12	El sistema provisionará una licencia de Exchange si el atributo de bandera de “EmailAccount Flag” está puesto como “Y”.
ONBRD-1.13	El sistema creará una auditoría y bitácora de los eventos realizados en el sistema para el nuevo usuario
ONBRD-1.14	El sistema creará una auditoria y bitácora de nuevos usuarios, transferencias, terminaciones y recontrataciones.
ONBRD-1.15	El sistema mandará una notificación al equipo de provisioning cuando se procese la creación de un usuario nuevo
ONBRD-1.17	EL sistema mandará un correo de notificación al equipo de Help Desk or Service Desk con el nombre completo y alias del nuevo usuario para que instalen la computadora y todo el hardware necesario para un usuario nuevo.

Flujo de trabajo de una terminación/Off-boarding

Esta sección describe los pasos del proceso que el sistema tomará para terminar el record de una identidad/usuario de los recursos de IDB

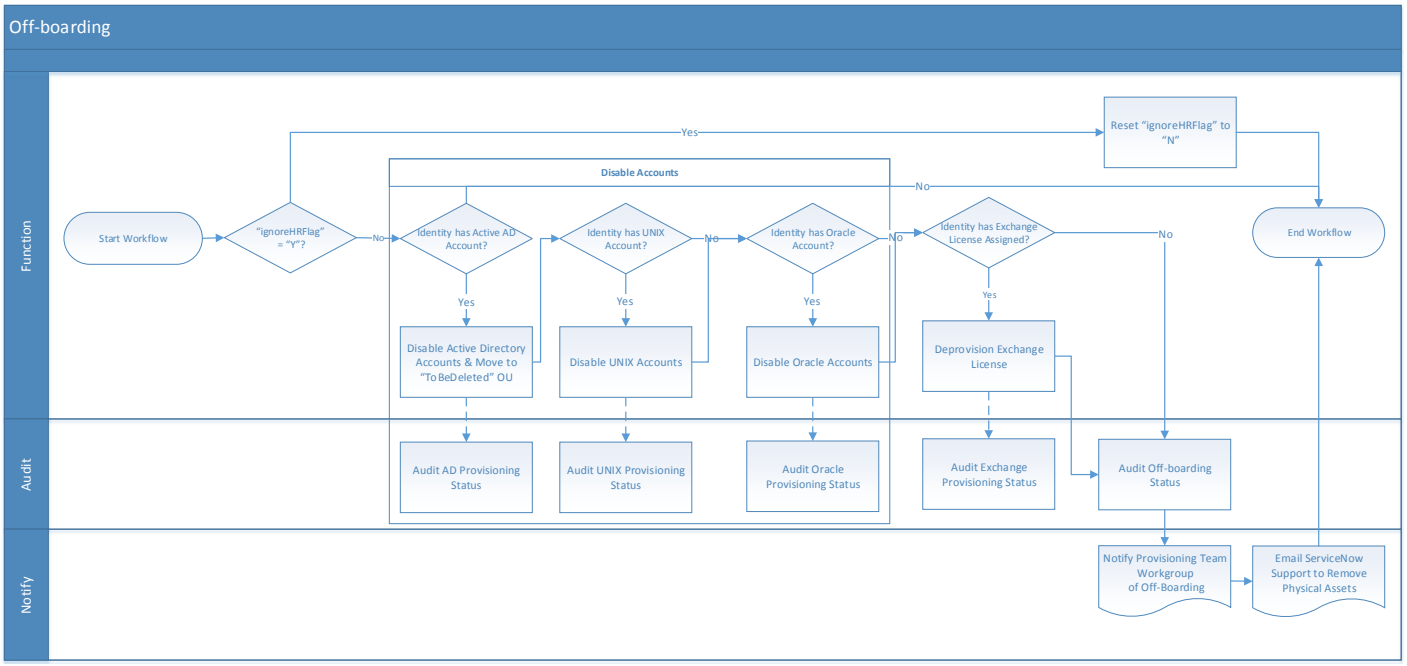


Figura 3: Flujo de trabajo de Terminación

Terminación/Off-boarding Requerimientos del usuario(ver tabla 14 y 15)

La suspensión de cuentas del usuario o terminación será iniciada después de que el contrato del usuario termine en People Soft(el sistema fuente de Recursos Humanos). El proceso de terminación iniciará cuando el estatus del record del usuario cambie en People Soft de “1” a “0”. El proceso manejará todo el deprovisionamiento de las ceuntas asociadas al usuario.

Las cuentas de aplicaciones que deshabilitará el sistema son las siguientes:

- Active Directory
- Exchange 365
- Oracle Database
- Control Minder (Unix)

Proposito: Este proceso asegurará identidades/usuarios inactivos sean propiamente terminados y las cuentas suspendidas y expiradas.

Suspuestos: No existen

46

Tabla 14 - Terminación/Off-boarding Requerimientos del usuario

NO REQ	REQUERIMIENTO FUNCIONAL
OFBRD-1. El sistema procesará la terminación de la entidad/usuario inhabilitando las cuentas especificas del usuario.	
OFBRD-1.1	El sistema inhabilitará la cuenta de Active Directory y las cuentas asociadas a la cuenta Global de la identidad/usuario. También inhabilitará la cuenta de correo electrónico en caso de que el usuario tenga alguna cuenta asociada
OFBRD-1.2	El sistema moverá la identidad/cuenta hacia la unidad(OU) 'ToBeDeleted' en Active Directory después de que la cuenta es suspendida.
OFBRD-1.3	Una vez que la cuenta de la identidad/Usuario se mueve a la OU 'ToBeDeleted' en Active Directory el buzon de correo electrónico es desconectado de la cuenta de active directory también todos los grupos que tiene la cuent de Active directory se remueven.
OFBRD-1.4	El sistema inhabilitará todas las cuentas de Oracle asociadas a la identidad.
OFBRD-1.5	El sistema inhabilitará todas las cuentas de Unix asociadas a la identidad.
OFBRD-1.6	El sistema creará una entrada de auditoria a continuación de la terminación de la cuenta de Active Directory por la terminación del usuario.
OFBRD-1.7	El sistema creará una entrada de auditoria a continuación del deslicenciamiento de la cuenta de Exchange por la terminación del usuario.
OFBRD-1.8	El sistema creará una entrada de auditoria a continuación de la suspensión de la cuenta de Oracle por la terminación del usuario.
OFBRD-1.9	El sistema creará una entrada de auditoria a continuación de la suspensión de la cuenta de Unix por la terminación del usuario.
OFBRD-1.10	El sistema creará una entrada de auditoria a continuación de la terminación del usuario.

47

NO REQ	REQUERIMIENTO FUNCIONAL
OFBRD-1.11	El sistema mandará una notificación de correo electrónico al equipo de provisioning después de la terminación de un usuario.
OFBRD-1.12	El sistema mandará una notificación de email al equipo de Service Desk/help desk después de la terminación de un usuario para remover los insumos de Hardware.
OFBRD-1.13	Los administradores pueden ototgar días de gracias manualmente a los usuarios que serán terminados el día que termina su contrato, pero el oficial de contratos solicitó 5 días de gracia para procesar el nuevo contrato, esto es una excepción.

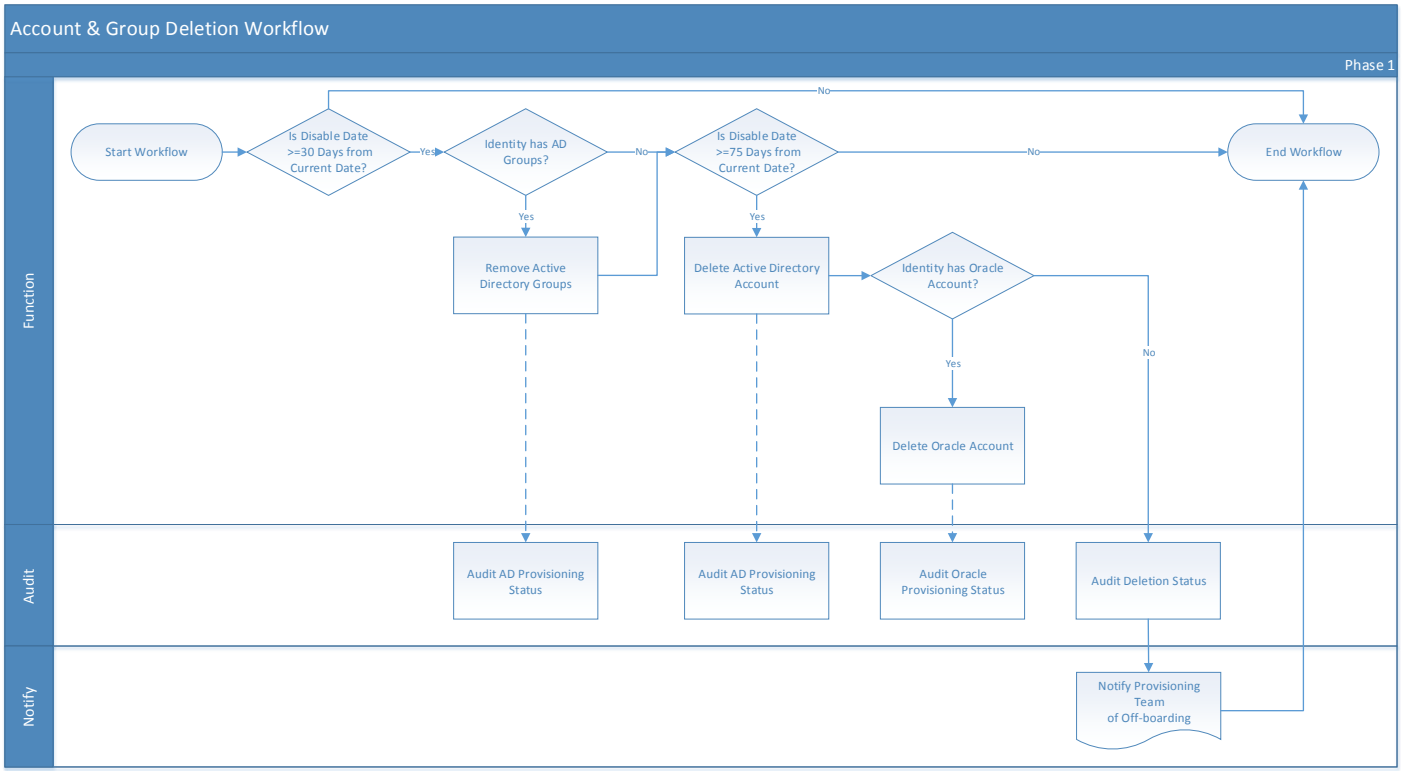


Figura 4: Flujo de Trabajo para borrar cuenta y grupo

Tabla 15 - Terminación/Off-boarding Requerimientos del usuario

NO REQ	REQUERIMIENTO FUNCIONAL
OFBRD-2. Los administradores harán una auditoria manual en donde encontraran cuentas de active directory activas y el sistema las terminará propiamente. La uaditoria se realizará cada 15 días.	

48

NO REQ	REQUERIMIENTO FUNCIONAL
OFBRD-2.1	El sistema removerá a la identidad/usuario de los grupos de Active Directory si la siguiente combinación es verdadera: Status = “0” AND Disable Date is >=30 Days from today but < 75 Days from today AND La cuenta de Active Directory está inhabilitada.
OFBRD-2.2	El sistema borrará la cuenta de Active Directory de la identidad/usuario si la siguiente combinación es verdadera: Status = “0” AND Disable Date is >=75 Days from today
OFBRD-2.3	EL sistema creará una entrada de auditoria recondando los detalles de la eliminación de la cuenta de active directory.
OFBRD-2.4	El sistema creará una entrada de auditoria del deprovisionamiento de las cuentas de Oracle para el usuario terminado.
OFBRD-2.5	El sistema creará una entrada de auditoria del deprovisionamiento de las cuentas de Unix para el usuario terminado.
OFBRD-2.6	El sistema notificará con un correo electrónico al equipo de provisioning sobre la terminación de la cuenta Global del usuario y de todas las cuentas que se encontraban dentro de su contenedor.

Flujo de trabajo de recontratación

Esta sección describe los pasos que el sistema tomará para manejar records de las identidades para las recontrataciones.

El flujo de trabajo de recontratación de un usuario del banco IDB que ha pasado de inactivo a activo en el sistema de recursos humanos People Soft se reactivará en el proceso de provisioning, el flujo de trabajo reactivará y provisionará las cuentas de Active Directory y Exchange. El sistema de provisioning mandará una notificación de correo electrónico a el área de Help desk para que asignes el hardware(Oficina, teléfono, computadora, etc.)

49

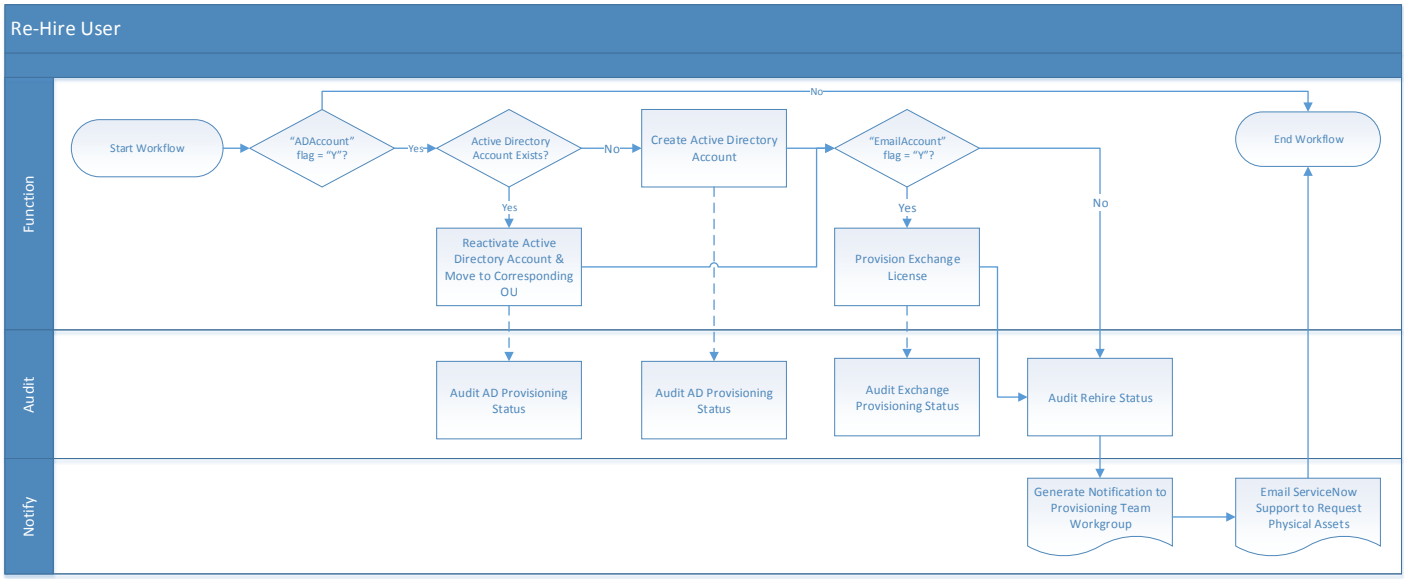


Figura 5: Flujo de trabajo de Recontratación

Requerimientos de recontratación de usuario(ver tabla 16)

Proposito: Reactivar cuentas inhabilitadas de Active Directory o crear cuentas nuevas para identidades recontratadas. Provisionar buzones de Exchange para identidades recontratadas.

Supuestos:

Los buzones de Exchange pueden ser restaurados solo si tienen 90 días de ser desconectados debido a una terminación. Un nuevo buzón de correo electrónico será provisionado si el usuario es recontratado después de 90 días de su terminación.

Tabla 16 - Requerimientos de recontratación de usuario

NO REQ	REQUERIMIENTO FUNCIONAL
RHIRE-1.	**El sistema reactivará las identidades recontratadas.**
RHIRE-1.1	El sistema reactivará la cuenta de Active Directory de la identidad/usuario recontratado.

NO REQ	REQUERIMIENTO FUNCIONAL
RHIRE-1.2	El sistema creará una nueva cuenta de Active Directory para la identidad/Usuario si las siguientes condiciones se juntan: 1) Si la bandera de provisioning de AD de la Identidad/Usuario es “Y” 2) Si la Identidad/Usuario no tiene actualmente una cuenta de Active Directory asociada.
RHIRE-1.3	El sistema provisionará un nuevo buzón de correo electrónico para la identidad/Usuario si las siguientes condiciones se juntan: 1) Si la bandera de provisioning de email account de la Identidad/Usuario es “Y” 2) Si la cuenta del usuario/identidad no tiene actualmente una cuenta asociada de Exchange.
RHIRE-1.4	El sistema creará una entrada de auditoria para el deprovisioning de la terminación de la cuenta de Active Directory del usuario/Identidad.
RHIRE-1.5	El sistema creará una entrada de auditoría para el deprovisioning de la terminación de la licencia de Exchange del usuario/Identidad.
RHIRE-1.6	El sistema creará una entrada de auditoria para guardar los detalles de provisioning del evento de re-hire del usuario/identidad.
RHIRE-1.7	El sistema notificará al grupo de trabajo provisioning team sobre el re-hire de la identidad.
RHIRE-1.8	El sistema enviará una notificación de email al equipo de trabajo de ¨ITE client center¨ para asignar los activos de hardware para el usuario recontratado.

Flujo de trabajo cuando un usuario es transferido de una unidad a otra.

La sección describe el proceso de los pasos que el sistema tomará para administrar la transferencia del usuario/identidad.

51

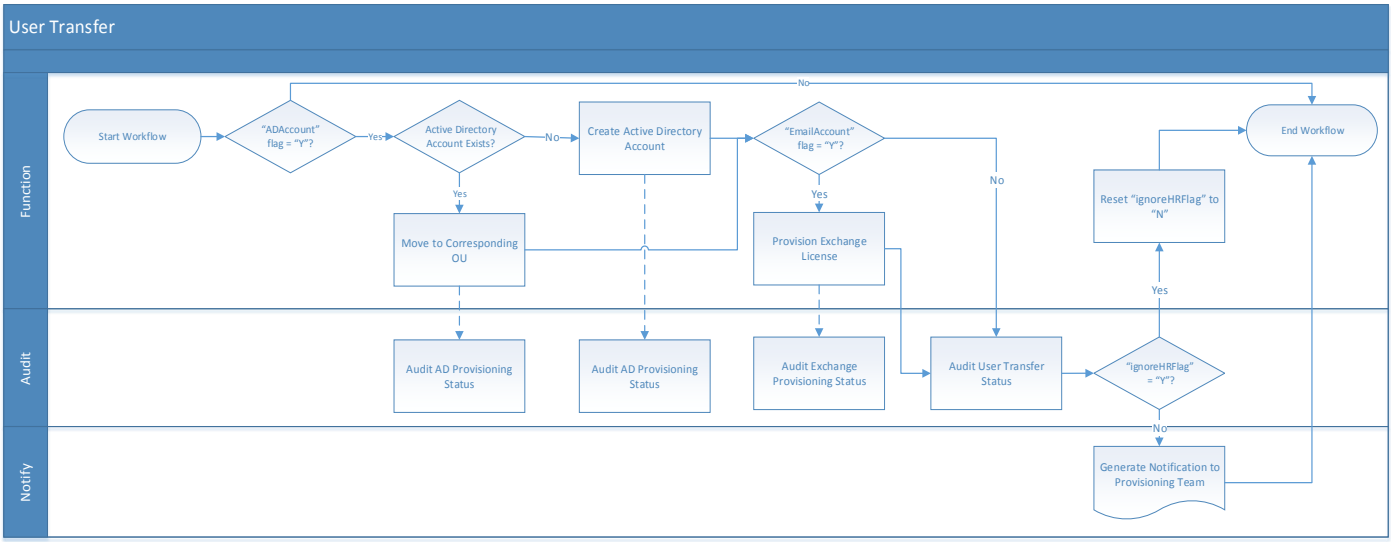


Figura 6: Flujo de trabajo de transferencia

Requerimientos de transferencia de usuario(ver tabla 17)

El flujo de trabajo de una transferencia manejará los cambios de un usuario de una unidad Organizacional a otra, las transferencias son iniciadas por el sistema fuente de recursos Humanos.

Las aplicaciones que serán afectadas por la transferencia son las listadas a continuación:

- Active Directory
  - Mover la cuenta de Active Directory a su nueva Unidad Organizacional
  - Modificación de los grupos que son por defecto

El sistema moverá las cuentas de una unidad organizacional a otra automáticamente mientras se encuentren en el mismo dominio, si la transferencia es de un dominio a otro el equipo de active directory moverá la cuenta manualmente.

Proposito: Para mover la cuenta de Active Directory de la identidad/usuario a la Unidad Organizacional apropiada basado en el cambio de departamento de la identidad/usuario.

Supuestos: Ninguno

52

Tabla 17 - Requerimientos de transferencia de usuario

NO REQ	REQUERIMIENTO FUNCIONAL
USTRN-1. El sistema manejará las transferencias de departamento de un usuario/identidad via el flujo de trabajo de una transferecnia.	
USTRN-1.1	El sistema automaticmente detectará un cambio de departamento en el record del usuario.
USTRN-1.2	El sistema creará una cuenta de Active Directory para la identidad/usuario si las siguientes condiciones se juntan: • La bandera de provisioning de AD es “Y” • La identidad/usuario no tiene una cuenta de Active Directory asociada
USTRN-1.3	El sistema provisionará un nuevo buzón de correo electrónico para la identidad/Usuario si las siguientes condiciones se juntan: • Si la bandera de provisioning de email account de la Identidad/Usuario es “Y” • Si la cuenta del usuario/identidad no tiene actualmente una cuenta asociada de Exchange.
USTRN-1.4	El sistema moverá la ceunta de AD de la identidad/usuario a la nueva unidad organizacional basado en el nuevo “Department ID” en el mismo dominio. (las cuentas que se tienen que mover en diferentes dominios se moverán manuelmente debido a la limitación del sistema en AD).
USTRN-1.5	El sistema generará una notificación cuando se procese la transferecnia de una unidad a otra y el equipo de provisioning hará las gestiones correspondientes para mover las cuentas que necesiten moverse de un dominio a otro. Las cuentas que se mueven en el mismo dominio se mueven automáticamente.
USTRN-1.6	El sistema no moverá las cuentas de Active Directory entre dominios durante el proceso de transfer.
USTRN-1.7	El sistema creará una entrada de auditoria con los detalles de la transfer.

53

NO REQ	REQUERIMIENTO FUNCIONAL
USTRN-1.8	El sistema creará una entrada de auditoria hacia la transferencia de la cuenta de Active Directory del usuario/identidad.
USTRN-1.9	El sistema creará una entrada de auditoria del licenciamiento de la cuenta de Exchange de la transferencia del usuario.

Flujo de trabajo de actualización de Usuario

La sección describe los pasos del proceso que el sistema tomará para administrar la actualización del usuario/identidad.

El flujo de trabajo de actualización de un usuario del banco IDB provisiona y desprovisiona cuentas del usuario de Active Directory y de Exchange basado en la coincidencia del estado de banderas de provisioning del usuario/identidad. La actualización del usuario será iniciada después de que People Soft actualice los datos de las banderas de provisioning.

54

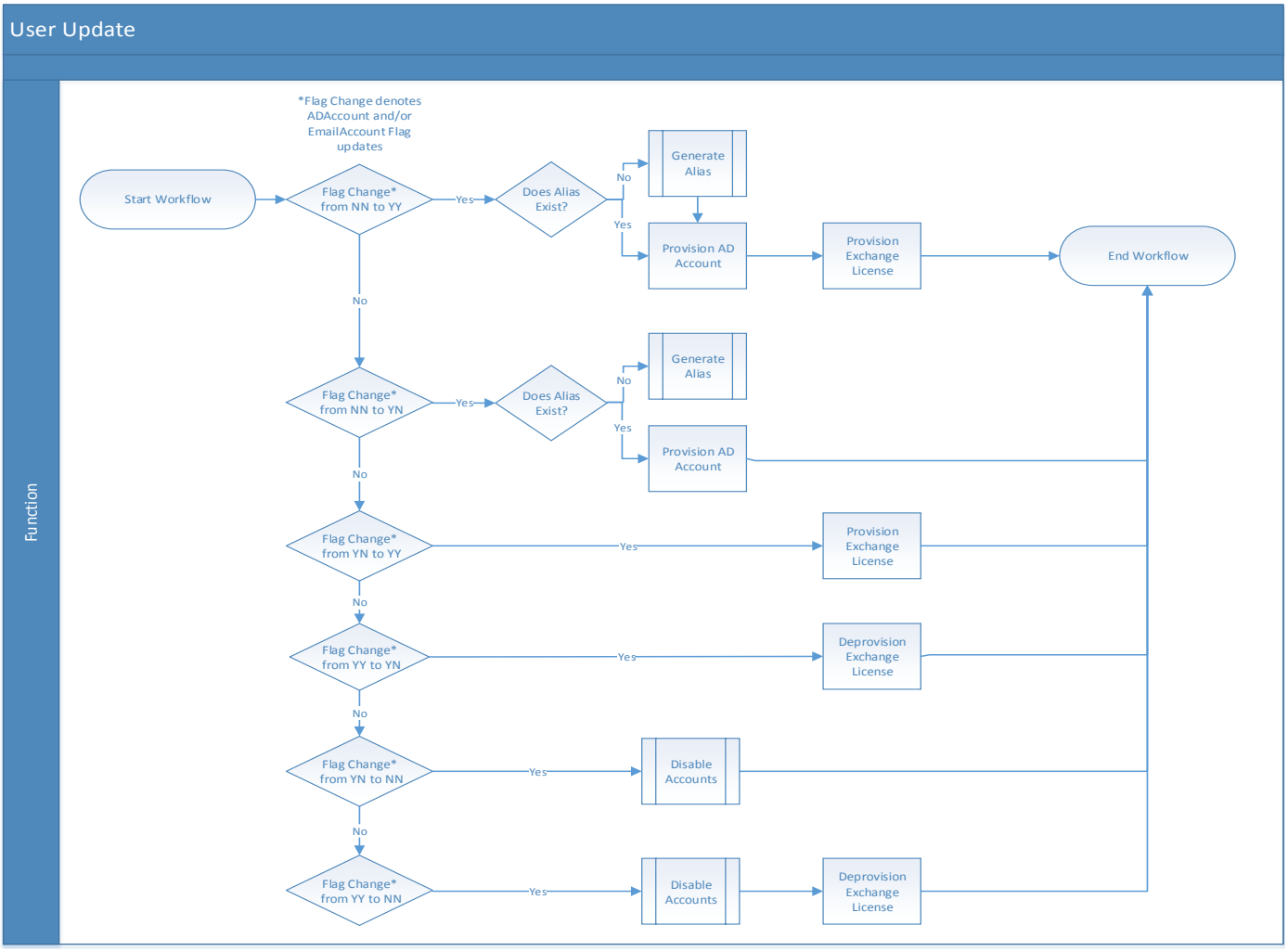


Figura 7: Flujo de trabajo para actualizar a un usuario

Requerimientos de actualización de usuario(ver tabla 18)

Proposito: El propósito es actualizar el acceso de la identidad basado en los cambios de bandera de la identidad/usuario de Active directory y/o correo electrónico.

Supuestos:

ninguno

Tabla 18 - Requerimientos de actualización de usuario

NO REQ	REQUERIMIENTO FUNCIONAL
USUPD-1.	**El sistema manejará las actualizaciones de los atirbutos de la identidad/usuario via el proceso del flujo de trabajo de la actualización del usuario.**

55

NO REQ	REQUERIMIENTO FUNCIONAL
USUPD-1.1	El sistema tomará la siguiente acción cuando los atributos “ADAccount” y “EmailAccount” cambien de bandera de “N|N” a “Y|Y”: • Generar un alias para el usuario si este no existe • Provisionar una cuenta de Active Directory • Provisionar licencia de Exchange • Generar notificación de correo electrónico para el equipo provisioning con un aviso de nuevo usu • ario/ onboarding
USUPD-1.2	El sistema tomará la siguiente acción cuando los atributos “ADAccount” y “EmailAccount” cambien de bandera de “N|N” a “Y|N”: • Generar un alias para el usuario si este no existe • Provisionar una cuenta de Active Directory • Generar notificación de correo electrónico para el equipo provisioning con un aviso de nuevo usuario/ onboarding
USUPD-1.3	El sistema tomará la siguiente acción cuando los atributos “ADAccount” y “EmailAccount” cambien de bandera de “Y|N” a “Y|Y”: • Provisionar licencia de Exchange
USUPD -1.4	El sistema tomará la siguiente acción cuando los atributos “ADAccount” y “EmailAccount” cambien de bandera de “Y|Y” a “Y|N”: • Desprovisionamiento de la licencia de exchange
USUPD -1.5	El sistema tomará la siguiente acción cuando los atributos “ADAccount” y “EmailAccount” cambien de bandera de “Y|N” a “N|N”: • Suspender cualquier cuenta de Active Directory, Oracle y Unix del usuario • Generar notificación de correo electrónico para el equipo provisioning con un aviso de Terminación de usuario/Off-boarding

56

NO REQ	REQUERIMIENTO FUNCIONAL
USUPD -1.6	El sistema tomará la siguiente acción cuando los atributos “ADAccount” y “EmailAccount” cambien de bandera de “Y|Y” a “N|N”: • Suspender cualquier cuenta de Active Directory, Oracle y Unix del usuario • Desprovisionamiento de la licencia de exchange • Generar notificación de correo electrónico para el equipo provisioning con un aviso de Terminación de usuario/Off-boarding

Administración de contraseñas(ver tabla 19)

Generación de contraseña

Proposito: El sistema generará una contraseña genérica para las cuentas de Active Directory, la cuál no será conocida por los usuarios finales, los usuarios finales tendrán que llamar con el equipo de Service Desk/Help Desk para solicitar una contraseña nueva.

El sistema generará una contraseña genérica para cada cuenta de usuario.

Supuestos: None

Tabla 19 - Administración de contraseñas usuario

NO REQ	REQUERIMIENTO FUNCIONAL
PWGEN-1. El sistema generará una contraseña genérica para las cuentas de Active Directory.	
PWGEN-1.1	El sistema requerirá una contraseña de al menos 10 caracteres de largo.
PWGEN-1.2	El sistema requerirá un password que contenga al menos tres de las siguientes caracteristicas • Letras mayúsculas (A-Z) • Letras minusculas (a-z) • Números (0-9) • Caracteres no alfa númericos (ej: !, $, #, or %)

57

Oracle(ver tabla 20)

Proposito: Cambio de contraseña de Oracle via el sistema de provisioning(IDM).

Suspuestos: Cambio de contraseña será via una cuenta de servicio de Oracle.

Tabla 20 - Oracle

NO REQ	REQUERIMIENTO FUNCIONAL
PWORA-1. Cambio de contraseña de Oracle via el sistema de provisioning(IDM).	
PWORA-1.1	El sistema permitirá a los Administradores del sistema de provisioning cambiar la contraseña de Oracle de los usuarios.
PWORA-1.2	El sistema requerirá un password de al menos 10 caracteres de largo.
PWORA-1.3	El sistema requerirá un password que contenga al menos tres de las siguientes caracteristicas • Letras mayúsculas (A-Z) • Letras minusculas (a-z) • Números (0-9) • Caracteres no alfa númericos (ej: !, $, #, or %)

58

UNIX(ver tabla 21)

Proposito: Cambio de contraseña de Unix via el sistema de provisioning(IDM) con la funcionalidad de Control Minder.

Supuestos: Password reset will be done via the custom Unix (Control Minder) connector

Tabla 21 - Unix

NO REQ	REQUERIMIENTO FUNCIONAL
PWUNX-1. Cambio de contraseña de Unix via el sistema de provisioning(IDM) con el conector Control Minder.	
PWUNX-1.1	El sistema permitirá a los Administradores del sistema de provisioning cambiar la contraseña de Unix de los usuarios.
PWUNX-1.2	El sistema requerirá un password de al menos 10 caracteres de largo.
PWUNX-1.3	El sistema requerirá un password que contenga al menos tres de las siguientes caracteristicas • Letras mayúsculas (A-Z) • Letras minusculas (a-z) • Números (0-9) • Caracteres no alfa númericos (ej: !, $, #, or %)

Notificaciones y Plantillas(ver Tabla 22)

Notificaciones administrativas

Notificación de activación de nuevo usuario

Proposito: Notificar al equipo de Provisioning, al equipo de email, al equipo de Service Desk la creación de un nuevo usuario.

Tabla 22 –Notificaciones y Plantillas

NO REQ	REQUERIMIENTO FUNCIONAL
NOTF-2. Creación de nuevo Usuario	

59

NO REQ	REQUERIMIENTO FUNCIONAL
NOTF-2.1	El sistema mandará un correo de notificación para el equipo de Provisioning, al equipo de email, al equipo de Service Desk sobre la creación de un nuevo usuario.
NOTF-2.2	Cuando un usuario/identidad completa el proceso de creación, el sistema mandará una notificación para el equipo de Provisioning, al equipo de email y al equipo de Service Desk basado en la plantilla de abajo.
Plantilla de correo: SUBJECT: New AD Account for **<Alias>** Created email notification from Identity Manager TEXT: Automatic Email from Identity Manager. ********** Create New User UserID:**<Alias>** FullName:<**LastName>,<FirstName>** EmployeeID:**<EmployeeID>** OrgUnit:**<DeptID>** User Type: **<UserType>**	

Notificación de Terminación de usuario(ver Tabla 23)

Proposito: Notificar al equipo de Provisioning, al equipo de email, al equipo de Service Desk la terminación de un usuario.

Tabla 23 – Notificación de Terminación de usuario

NO REQ	REQUERIMIENTO FUNCIONAL
NOTF-3.	**Terminación de Usuario**
NOTF-3.1	Cuando una identidad/Usuario es terminado. El sistema mandará un correo de notificación para el equipo de Provisioning, al equipo de email, al equipo de Service Desk sobre la terminación de un usuario.

60

NO REQ	REQUERIMIENTO FUNCIONAL
	Plantilla de correo: SUBJECT: User **<Alias>**Terminated email Notification from Identity Manager TEXT: Automatic Email from Identity Manager. ********** Terminate User UserID:**<Alias>** LastName:**<LastName>** FirstName:**<FirstName>** IDNo.:**<EmployeeID>** OrgUnit:**<DeptID>** User Type: **<UserType>**

Notificación de recontratación(ver Tabla 24)

Proposito: Notificar al equipo de Provisioning, al equipo de email, al equipo de Service Desk la Recontratación de un usuario.

Tabla 24 –Notificación de recontratación

NO REQ	REQUERIMIENTO FUNCIONAL
NOTF-4.	**Recontratación de Usuario/identidad**
NOTF-4.1	Cuando una identidad/Usuario es recontratado. El sistema mandará un correo de notificación para el equipo de Provisioning, al equipo de email, al equipo de Service Desk sobre la recontratación de un usuario.

61

NO REQ	REQUERIMIENTO FUNCIONAL
	Plantilla de correo: SUBJECT: User <Alias> Re-Hire Email Notification from Identity Manager TEXT: Automatic Email from Identity Manager. ********** Rehired User UserID:**<Alias>** LastName:**<LastName>** FirstName:**<FirstName>** IDNo.:**<EmployeeID>** OrgUnit:**<DeptID>** User Type: **<UserType>**

Notificación de transferencia(ver tabla 25)

Proposito: Notificar al equipo de Provisioning, al equipo de email, al equipo de Service Desk cuando el departamento(Org Unit) de un usuario cambia.

Tabla 25 –Notificación de transferencia

NO REQ	REQUERIMIENTO FUNCIONAL
NOTF-5.	**Transferencia de departamento(Org Unit) del usuario**
NOTF-5.1	Cuando el “Department ID" de un usuario cambia y el evento de una transferencia es procesado, el sistema mandará una notifiación de correo electrónico al equipo de Provisioning, al equipo de email, al equipo de Service Desk basado en la plantilla de abajo.
NOTF-5.2	Cuando los tres caracteres del “Department ID” de la identidad/usuario es igual a un código de un país del dominio REG el subject del correo iniciará con “REG”, de lo contrario iniciará con “User”.

62

NO REQ	REQUERIMIENTO FUNCIONAL
	Plantilla de correo: SUBJECT: (User **OR** REG) <Alias> Transfer Email Notification from Identity Manager TEXT: Automatic Email from Identity Manager. ********** Transfer User UserID:**<Alias>** LastName:**<FirstName>** FirstName:**<LastName>** IDNo.:<**EmployeeID>** PreviousOrgUnit:**<DeptID>** NewOrgUnit:**<DeptID>** User Type: **<UserType>**

Provisioning(ver Tabla 26)

Tabla 26 – Provisioning

NO REQ	CASO DE USO	REQUERIMIENTOS DEL NEGOCIO – ADMINISTRACION DE CICLO DE VIDA DE UN USUARIO
RN.5	Active Directory	El sistema estará disponible para conectar con los dominios de active directory del Banco(IDB) y provisionar a los usuarios con cuentas y grupos. Una política mapeara a los usuarios en el active directory en la Org/Unit(Unidad Organizacional) que le corresponde de acuerdo a su contrato con RH. Las dominios de Active Directory están divididos por carpetas de (Org/Units)unidades Organizacionales de todo el banco.

63

NO REQ	CASO DE USO	REQUERIMIENTOS DEL NEGOCIO – ADMINISTRACION DE CICLO DE VIDA DE UN USUARIO
RN.6	Office 365	El sistema estará disponible para provisionar office 365(Exchange) con la licencia de correo del usuario. El deslicenciamiento será ejecutada con la terminación/suspensión del usuario. Cuando el usuario es terminado/suspendido la cuneta de Active Directory se mueve a un contenedor llamado ToBeDeleted en donde el buzon de correo electrónico es desprendido de la cuenta de Active Directory y se le remueve la licencia de correo.
RN.8	People Soft HR	El sistema estará disponible para conectar con People Soft para leer los datos del usuario y escribir el email address y user ID del usuario en el perfil de people soft del usuario. People Soft es la aplicación fuente para el sistema de provisionamiento.
RN.9	Oracle	El sistema estará disponible para conectar con Oracle y provisionar cuentas, perfiles, roles para usuarios y privilegios de sistema.
RN.10	UNIX	El sistema estará disponible para conectar y provisionar cuentas de usuario y grupos de Unix via un conector de CA Control Minder
RN.11	ServiceNow	El sistema estará disponible para generar notificaciones de email para integrar con el sistema ServiceNow para generación de tickets.

Reporteo y Auditoria(ver tabla 27)

64

Tabla 27 – Reporteo y Auditoria

NO REQ	CASO DE USO	REQUERIMIENTOS DEL NEGOCIO – ADMINISTRACION DE CICLO DE VIDA DE UN USUARIO
RN.12	Reporteo y Auditoria	Los administradores serán capaces de utilizar los resportes y auditorias del sistema para obtener datos y logs históricos(i.e. provisionamiento de usuarios durante un periodo, accesos actuales del usuario en todos los end points(aplicaciones) que el sistema administra). Auditoria de logs se configura para capturar eventos procesados en el sistema.

Administración de contraseñas(ver tabla 28)

Tabla 28 – Administración de contraseñas

NO REQ	CASO DE USO	REQUERIMIENTOS DEL NEGOCIO
RN.13	Cambio de contraseña en Oracle	Los administradores serán capaces de realizar cambios de contraseña de cuentas de Oracle desde la aplicación de provisioning Manager(PM). No es necesario ingresar a la consola de ODBC de Oracle para realizar el cambio de contraseña.
RN.14	Cambio de contraseña en Unix	Los administradores serán capaces de realizar cambios de contraseña de cuentas de Unix via Control Minder integration
RN.15	Complejidad del contraseñas	Para cada sistema/aplicación que se agregue para ser administrado por el sistema IDM, Provisioning Manager(PM), tendrá que cumplir con las políticas de complejidad de contraseñas que el banco interamericano de desarrollo utiliza para sus controles internos

- Provisionamiento de usuarios en lote, esto quiere decir que el sistema puede procesar diferentes eventos de provisionamiento(nuevos usuarios, reactivación, supencion de usuarios y transferencias) en una sola ejecución.

65

- Creación de cuentas de correos electrónico de la organización
- Administración de Active Directory
- Administración de cuentas de usuario de Oracle
- Administración de cuentas de usuario de Unix
- Creación de Templates y roles

66

Flujo de trabajo del Provisioning process

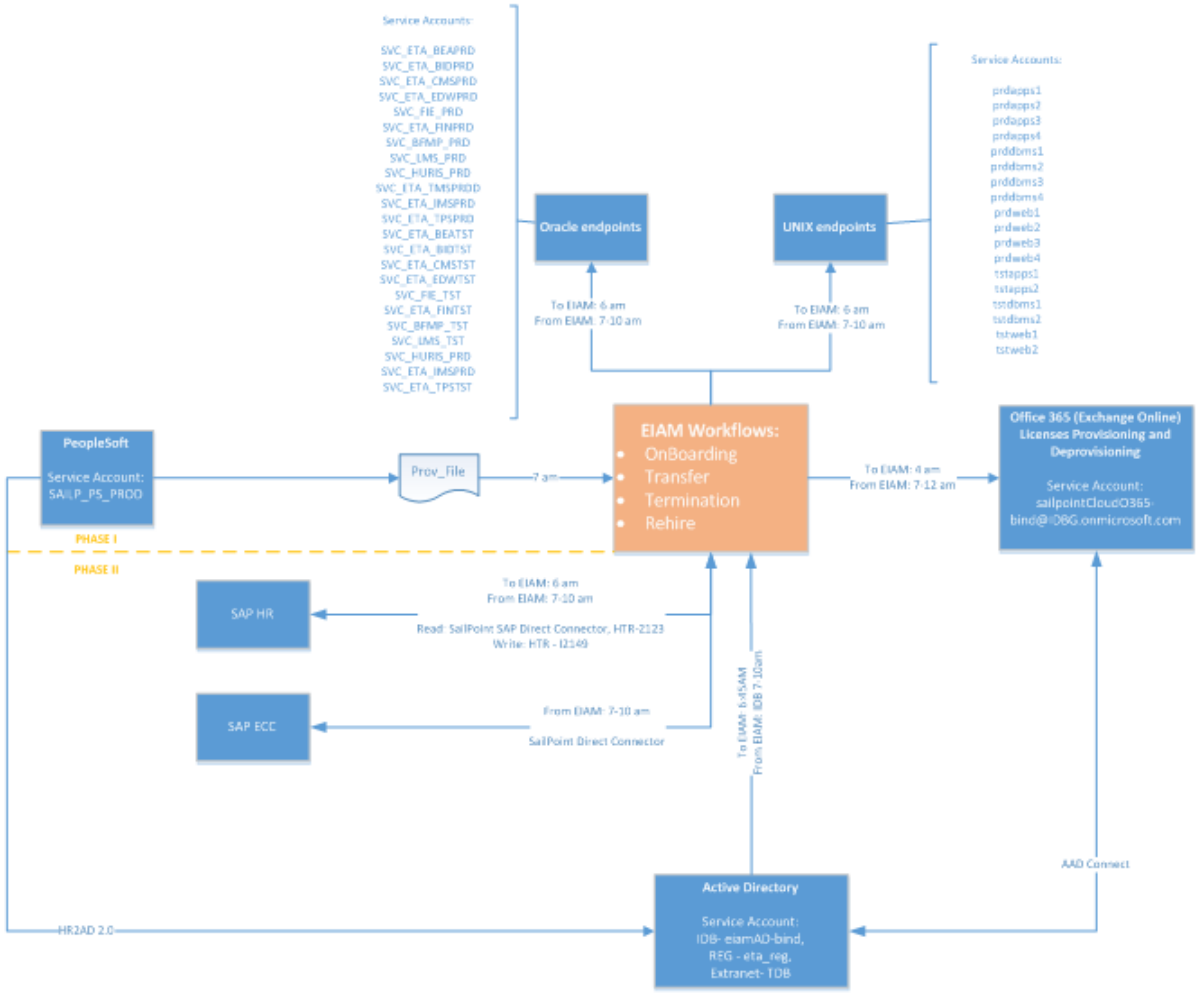


Figura 8: Flujo de trabajo del Provisioning process

67

1.13 Plantillas de Notificación de email

1.13.1 Lógica de notificacion de email

Correos específicos de cada flujo de trabajo del usuario(creación de nuevo usuario, terminación, transferencia y recontratación) serán iniciados por los cambios de estatus de recursos humanos en People Soft

1.13.2 Plantillas de notificaciones email

La sección de abajo resume las plantillas especificas de cada flujo de trabajo y sus recipientes.

1.13.3 Plantilla de creación de usuario nuevo

cuando un nuevo usuario es creado(new user) el siguiente correo es enviado

```
From eiamdev-noreply@iadb.org
To:          sqainfosec@iadb.org,          etrustadmin@iadb.org,
helpdesk@iadb.org, EMAILGROUP@iadb.org, iadb@service-now.com

Subject: New AD Account for TUSER Created email notification
from Identity Manager

Automatic Email from Identity Manager
**********************************************************
******
     Onboarded User

               UserID: TUSER
               Last Name: Test
               First Name: User
               ID No.: 66611112
               Org Unit: EXD/013
               User Type: Contractual
               Point of Contact:
```

Nota: el equipo de Service desk helpdesk@iadb.org recibirá el correo solo si el miembro es de HQ. Sino lo es, el soporte técnico de cada país recibirá el correo de notificación.

1.13.4 Plantilla de Transfer

Cuando un usuario es transferido(DeptID cambia) el siguiente correo es enviado

```
From eiamdev-noreply@iadb.org
To:          sqainfosec@iadb.org,          etrustadmin@iadb.org,
helpdesk@iadb.org, EMAILGROUP@iadb.org, ITECOMPLIANCE@iadb.org,
opus_support@iadb.org, iadb@service-now.com


Subject: User TUSER Transfer Email Notification from Identity
Manager

Automatic Email from Identity Manager
************************************************************
******
     Transfer User

               UserID: TUSER
               Last Name: Test
               First Name: User
               ID No.: 66611112
               Org Unit: EXD/013
               User Type: Contractual
               Point of Contact:
               Office:
```

Nota: el equipo de Service desk helpdesk@iadb.org recibirá el correo solo si el miembro es de HQ. Sino lo es, el soporte técnico de cada país recibirá el correo de notificación

1.13.5 Plantilla Recontratación

Cuando un usuario es recontratado(estatus cambia de 0 a 1) el siguiente correo será enviado:

```
From eiamdev-noreply@iadb.org
To:          sqainfosec@iadb.org,          etrustadmin@iadb.org,
helpdesk@iadb.org, EMAILGROUP@iadb.org, iadb@service-now.com


Subject: User TUSER Re-Hire Email Notification from Identity
Manager

Automatic Email from Identity Manager
**********************************************************
******
     Rehired User
               UserID: TUSER
               Last Name: Test
               First Name: User
               ID No.: 66611112
               Org Unit: EXD/013
               User Type: Contractual
```

Nota: el equipo de Service desk helpdesk@iadb.org recibirá el correo solo si el miembro

es de HQ. Sino lo es, el soporte técnico de cada país recibirá el correo de notificación

Cuando un usuario es recontratado(estatus cambia de 0 a 1) y no tenía previamente una cuenta de Active Directory, el proceso de un usuario nuevo se llevará acabo.

1.13.6 Plantilla de Terminación

Cuando un usuario es Terminado(cambio de estatus de 1 a 0) el siguiente correo será enviado

```
From eiamdev-noreply@iadb.org
To:          sqainfosec@iadb.org,          etrustadmin@iadb.org,
helpdesk@iadb.org, EMAILGROUP@iadb.org, ITECOMPLIANCE@iadb.org,
TelecomSupportGroup@iadb.org, iadb@service-now.com

Subject: User TUSER Terminated Email Notification from Identity
Manager

Automatic Email from Identity Manager
************************************************************
******    User Off-boarding

               UserID: TUSER
               Last Name: Test
               First Name: User
               ID No.: 66611112
               Org Unit: EXD/013
               User Type: Contractual
               Point of Contact:
               Office:
```

1.13.7 Actualización de usuario

Hay dos casos de uso que enviarán correos de notificación

Cuando las banderas de provisioning de un usuario cambian de Y a N en Active Directory, los correos de notificación de creación de usuario nuevo serán enviados(referencia en la sección de Nuevo usuario/onboarding)

Cuando las banderas de provisioning de un usuario cambian de N a Y en Active Directory, los correos de notificación de Terminación de usuario serán enviados(referencia en la sección de Terminación/Offboarding)

Email Groups

Onboarding Notification Group

- <código de país>TechSup@iadb.org o Helpdesk@iadb.org (para la sede en HQ)
- SQAINFOSEC@iadb.org,
- EMAILGROUP@iadb.org,

Off-boarding Notification Group

- < código de país >TechSup@iadb.org o Helpdesk@iadb.org (para la sede en HQ)
- EMAILGROUP@iadb.org
- SQAINFOSEC@iadb.org,

Transfer Notification Group

- < código de país >TechSup@iadb.org (country member) o Helpdesk@iadb.org (para la sede en HQ)
- sqainfosec@iadb.org
- EMAILGROUP@iadb.org

72

ReHire Notification Group

- < código de país >TechSup@iadb.org (country member) o Helpdesk@iadb.org (para la sede en HQ)
- sgainfosec@iadb.org
- EMAILGROUP@iadb.org

5. Glosario

Negocio común o terminología especial no definida arriba es descrita en la siguiente tabla(ver tabla 29).

Tabla 29 – Glosario

TERMINOS GLOSARIO	DEFINICIÓN
IAM	Identidad y administración de accesos
IDM	Administración de Identidades
certificación/ certificación de Accesos/ Revisión de accesos/ Recertificación	El proceso de automatizar la revisión periódica y aprobación de accesos para los sistemas apropiados
Campaña certificación	Finalización de multiple certificaciones iniciales al mismo tiempo
Revisor/revisor certificación/certificador	Persona responsable para completar la revisión de un acceso
Revisor delegado	Usuario que ha sido asignado la revisión de un acceso por un revisor certificación
Solicitud de acceso	Sistemas o procesos usados para solicitar un acceso nuevo, hacer cambios a accesos existentes o remover accesos a recursos de una organización
Permiso	Un valor especifico para el atributo de una cuenta, comúnmente membresía de un grupo o un permiso

73

Administración del ciclo de vida	El proceso de ciclo de vida administra el acceso de un usuario durante su estancia en una organización
Provisioning	El proceso de otorgar, asignar, cambiar o remover accesos de usuarios en los sitemas, aplicaciones y bases de datos basados en una identidad única
Reporte	Un tipo de tarea que extrae información de la base de datos de IDM y presenta este con una opción de exportarlo a PDF y/o CSV

74

6. **Funcionalidad requerida**(ver tabla 30)

Tabla 30 – Funcionalidad requerida

#	Descripción	Soportado por la aplicación	
		Si	No
1	Proporcionar una arquitectura unificada de identidades y acceso de gestión con los servicios IAM que pueden ser aprovechados para administrar la capacidad de la población de usuarios del BID (aprox. 4500 usuarios finales).	✓	
2	Alta disponibilidad y capacidad de continuar proporcionando el soporte inenterrumpido en caso de un evento de desastre	✓	
3	Proporcionar herramientas o interfaces para la seguridad de TI de fácil uso, seguro y personal de apoyo para la gestión de acceso de usuarios o de identidad en tiempo real.	✓	
4	Proporcionar acceso basado en roles para administrar la aplicación y para conceder la administración distribuida para diferentes tipos de funciones de apoyo.	✓	
5	Proporcionar solicitudes de self-service seguras para 4500 usuarios internos + 2500 clientes externos para facilitar cuenta y solicitud de acceso, la aprobación y el aprovisionamiento a los sistemas gestionados por la aplicación.	✓	
6	Proporcionar una funcionalidad de flujo de trabajo, escalaciones/prioridades, excepciones, notificaciones por correo electrónico, aprobación, rechazo, escalada, recordatorios, para apoyar solicitudes de self-service y de revisión de acceso.		X
7	Proporcionar funcionalidad de control de acceso basado en roles para las composiciones de rol en el negocio.	✓	

75

	Funcionalidad para usar el atributo de asignación de rol de acuerdo a las actividades de negocio del usuario.		
8	Proporcionar el rol de ejercicio de minería para desarrollar el rol requerido para la estrategia del negocio y su implementación.		X
9	Proporcionar una visión única de la identidad del usuario en el directorio coorporativo con racionalización de multiples IDs para usuarios y clientes.	✓	
10	Proporcionar funcionalidad de administración distribuida basada en roles para el acceso a los sitemas.	✓	
11	Proporcionar una identidad única y central en todos los sistemas y checar si el usuario no existe en el repositorio del historial de usuarios		X
12	Funcionalidad de gestión de accesos para proporcionar un modelo central de autenticación basado en políticas de riesgo, single sign on	✓	
13	Adquirir infraestructura de sistemas para manejar sistemas como Active Directory, Microsoft Exchange 2010 para provisionar cuentas de dominio y buzones de correo electrónico, también manejar permisos en línea con la integración de RH	✓	
15	Adquirir sistemas de infraestructura como sistemas gestionados tales como Oracle ver.10.2 and 11 base de datos para provisionar cuentas y autorizaciones.	✓	
16	Adquisición de sistemas de infraestructura como sistemas gestionados tales como Unix AIX para provisionar cuentas y manejar grupos, grupos de recursos y permisos por medio de la integración de CA Control Minder.	✓	
17	Adquirir SAP ERP systems (ECC, SRM, BW, GRC, Solution Manager, Portal, CUA) como sistemas gestionados para provisionar cuentas y autorizaciones.		X
18	Adquirir el sistema operativo como sistema administrado para gestionar identidades y grupos de seguridad de SharePoint para provisionar un rol base de accesos utilizando atributos que		X

76

	aprovechan las funciones de todos los sistemas administrados, incluhyendo aplicaciones heredadas.		
19	Adquirir aplicaciones heredadas como sistemas gestionados tales como sistema de gestión de préstamos ”LMS”, sistema de gestión de la tesorería “TMS”. CMM, FIE, PeopleSoft HR, etc. Para provisionar cuentas y gestión de autorizaciones en el alcance de la organización de accesos basado en roles incluido acceso basado en atributo.		X
20	Automatizar el proceso de integración del usuario entre el provisioning process y el sistema de fuente de recursos humanos tales como People Soft o SAP HR		X
21	Solicitud de acceso de Self Service y de un componente de manejo de cuenta para la población de usuarios internos con flujo de trabajo para aprobaciones y aliniamientos con la arquitectura móvil del banco.		X
23	Servicio de manejo de contraseñas por el mismo usuario(Self Service) para toda la población de usuarios que se alinien con la arquitectura móvil del banco. Incluido reset de contraseñas de cuentas administradas por la población de usuarios pertinente. Incluya detalles del proceso de despliegue y el mecanismo para automatizar la generación de contraseñas aleatorias y rotación periódica.		X
24	Funcionalidad de acceso basado en roles para definir los roles empresariales compuestos por roles relevantes de aplicaciones, perfiles, grupos, clases, etc. de gestión de aplicaciones/sistemas. Además, atributo y regla de asignación basado en la función del role empresarial, así como la composición del role del negocio tambien funciones de roles base de aplicaciones individuales.	✓	
25	Componente de análisis de riesgo para revisar riesgos de acceso basado en un set de reglas de separación de funciones “SOD” y reglas de riesgo de procesos identificados en el negocio como riesgos y mejores practicas. Análisis de riesgos proactiva de las solicitudes de acceso del usuario y el proceso de asignación de funciones. Analisis de remediación de riesgos, conjunto de reglas para el manejo y asignación de controles para la mitigación de riesgos.		X

77

26	Reporte y análisis de riesgo de accesos, administración de funciones del negocio y gestión de acceso de los usuarios. Informe para las solicitudes de acceso, incluyendo el nivel de servicio para las solicitudes y peticiones con los conflictos y mitigación entre otros. Informes de seguridad para usuarios, grupos, roles y perfiles, etc. Reportes de auditoria relacionados sobre roles y cambios de asignación. Reporte de revisión de accesos basado en usuario, grupo de Active Directory, sistema/aplicación, unidad organizacional, recertificación, etc.		X
27	Exportar reportes a otros formatos: Excel, csv, xml, pdf, etc.	✓	
28	Componente de revisión de accesos automatizado para administrar la recertificación de accesos de los usuarios y también la configuración del role de recertificación de agregar vista del usuario. La capacidad de procesar por usuario, por sistema o por grupo de usuarios con un flujo de trabajo de aprobación en tiempo real o programado para proceso periódico.		X
29	Funcionalidad de acceso de superusuario con capacidades de vigilancia y control	✓	
30	Integración con multi-dominio de Microsoft Windows Active Directory para gestionar a los accesos de los usuarios internos del banco interamericano de desarrollo y autenticación en una infraestructura de acceso centralizada.	✓	
31	Integración con multi-dominio de Microsoft Windows Active Directory para gestionar el acceso de usuarios externos y autenticación en una infraestructura de acceso centralizada.	✓	
32	Integración con soluciones comerciales de autenticación con passwords robustos como RSA Secure ID y Entrust Identity Guard como parte de la de la arquitectura centralizada de accesos y tambien la administración del sistema de provisionamiento de hardware tokens.		X

78

33	Integracion con CA Site Minder para la autenticación centralizada y acceso a las aplicaciones Web.	✓	
34	Proporcionar rastreo de auditoria, monitoreo de todas las actividades realizadas en el sistema por los administradores y por los usuarios que intentan autenticarse usando una cuenta de altos privilegios	✓	
36	Integración con el sistema de reporteo por ejemplo Service now.		X
37	Soportar la integración con RSA enVision, por lo tanto, los registros de auditoria y de actividad puedan ser enviados a enVision para la presentación de informes.		X
39	Ligar todas las cuentas de un usuario a su usuario global(contenedor) administrada por la aplicación.	✓	
40	Automatizar el proceso de terminación, el sistema necesita automatizar el bloqueo y suspensión de todas las cuentas del usuario al momento de su terminación de contrato, también las cuentas necesitan ser suspendidas cuando el usuario cambie de banderas de provisioning de YY a NN		X
41	Realizar el proceso de transfer automáticamente, cuando el usuario es transferido de una unidad a otra el sistema debe mover la cuenta de Active Directory a la nueva unidad del usuario y generar el ticket para realizar la recertifacion de accesos		X
43	Cuando un usuario es recontratado las únicas cuentas que se deben de reactivar son las de active directory y la de correo electrónico	✓	
44	Funcionalidad de reconectar los mailboxes		X
45	Funcionalidad de obtener las estadísticas de cuantos eventos se han procesado de creación de usuarios, transferencias, recontrataciones y terminaciones de usuarios		X
46	Funcionalidad de actualizar automáticamente el status del empleado cuando el usuario es transicionado de non-staff a staff y viceversa		X

79

7. **Casos de Uso**(ver Tabla 31)

Las tablas siguientes describen los requisitos del negocio para el sistema EIAM

Requerimientos del negocio

Administración ciclo de vida

Tabla 31 –Casos de Uso

NO. REQ	CASO DE USO	REQUERIMIENTOS DEL NEGOCIO – ADMINISTRACION DE CICLO DE VIDA DE UN USUARIO
RN.1	Creación de cuenta de usuario nuevo	Cuando un usuario es ingresado en el sistema de recursos humanos (PeopleSoft), el sistema creara una identidad(basada en el numero de empleado) para el usuario y tambien lo creara en las aplicaciones apropiadas conectadas al sistema(Active directory, Exchange365, service now, mandar un correo para hacer la solicitud de pc, teléfono y oficina)
RN.2	Recontratación creación de cuenta	Cuando una recontratación es ingresada en el sistema de recursos humanos(People soft), el sistema EIAM agregará la información y reactivara la cuenta del usuario en Active directory y aplicaciones conectadas. Si una cuenta de active directory ya no existe para el usuario recontratado, el sistema creara una cuenta nueva en Active Directory y en exchange365 bajo el mismo alias
RN.3	Transferecnia de Usuario	Cuando un usuario es transferido de área(por ejemplo de Ciencias Naturales a Informatica) el sistema agregara la información de transferencia del sistema de recursos humanos (People Soft) y moverá la cuenta del usuario en el active directory hacia la Unidad Organizacional(UO) asignada, basada en la (UO) del usuario
RN.4	Terminación de Usuario	Cuando un usuario es terminado por el sitema de de recursos humanos(People Soft), el sistema actualizará la información y suspenderá las cuentas del usuario

80

Proceso de PSFEED(Proceso de provisionamiento)

Provisionamiento de las cuentas del banco Interamericano de Desarrollo en los dominios de active directory IDB y REG, es manejado por las cuentas administrativas via el proceso de PSFEED el cual procesa los siguientes eventos:

- Nuevo Usuario
- Terminación de usuarios
- Recontrataciones de usuarios
- Transferencia de usuarios
- Actualización de usuarios globales

Cada evento es aplicable para ambos tipos de usuario, staff y non-staff. El equipo de seguridad de la información(INFOSEC) recibe diariamente los records de provisionamiento de cada evento de acuerdo a la lógica procesada en el paquete SSIS, todos los records que son ingresados en el paquete tienen la siguiente estructura:

UserName|*FullName*|*FirstName*|*LastName*|*MiddleName*|*employeeID*|*EnableDt*|*DisableDt*|*DeptId*|*Title*|*Company*|*Phone*|*PrimaryMail*|*ManagerId*|*ManagerUserName*|*Status*|*PreferredFirstName*|*Location*|*DeptDescr*|*EmpldRcd*|*StreetAddress*|*City*|*State*|*PostalCode*|*Country*|*UserType*|*ADAccount*|*Email Account*|*AlternateEmplid*

El total del extracto de los records de los empleados (prov_file.txt) de PeopleSoft es respaldado en el siguiente share drive \\itfectp07\ el cual se respalda diarimente y se renombra con la convención *prov_file-MM-DD-YY.txt*.

Cada record recibido es analizado, revisado y documentado en un correo electrónico llamado PSFEED fechaMMDDYYYY

Para el propósito de reconciliación de datos del usuario, el equipo de provisioning recibe notificaciones en el buzon de INFOSEC de la colaboración de los siguientes equipos:

- Notificaciones de staff y Non-staff de acciones realizadas por el equipo de recursos humanos el día anterior, estas notificaciones son enviadas por el personal de recursos humanos.

81

Estas acciones deberán incluirse en correo de PSFEED por el oficial de securidad de la información que raliza el provisioning.

Los pasos de revisión y procesamiento son descritos a continuación.

Revisión

Usuarios nuevos

Accesar al servidor *HQPAPROVN* y navegar a los directorios *D:\psfeed\output\STAFF*, *D:\psfeed\output\NONSTAFF* y *D:\psfeed\output\EXCEPTIONS*.

Copiar la información de los siguientes archivos *new_users_role.csv* para Staff y *new_users_role_nonstaff.csv* para Non-staff dentro del correo de PSFEED en el apartado NEW_USERS_ROLE.

Copiar la información de *New_Users_Exception.csv*, *username_exception.csv* y *Role_Dept_Missing_Exception.csv*, dentro del correo de PSFEED en el apartado EXCEPTIONS.

NOTA

Casi siempre, los records guardados en el archivo *username_exception.csv* son el resultado de las cinco opciones de la lógica del alias name.

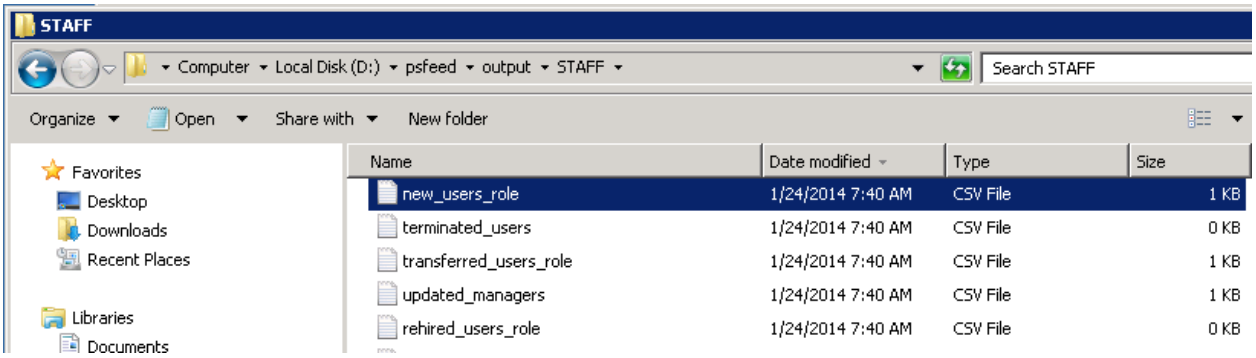


Figura 9: Nuevo Usuario

82

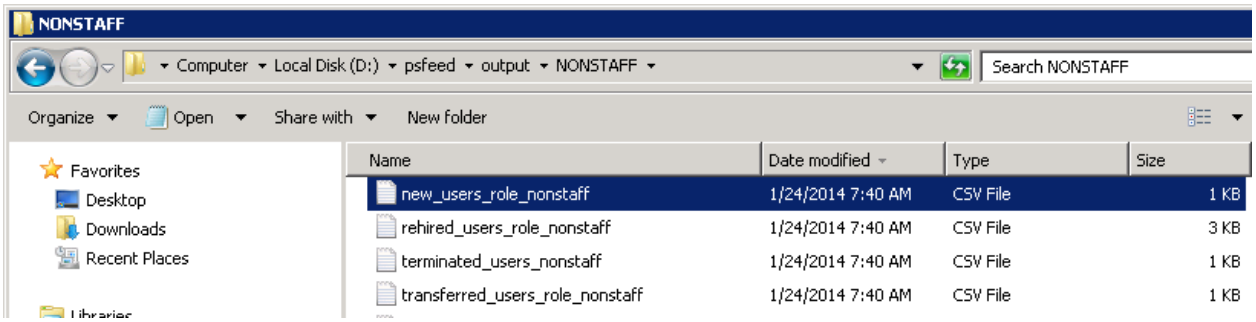


Figura 10: Nuevo Usuario

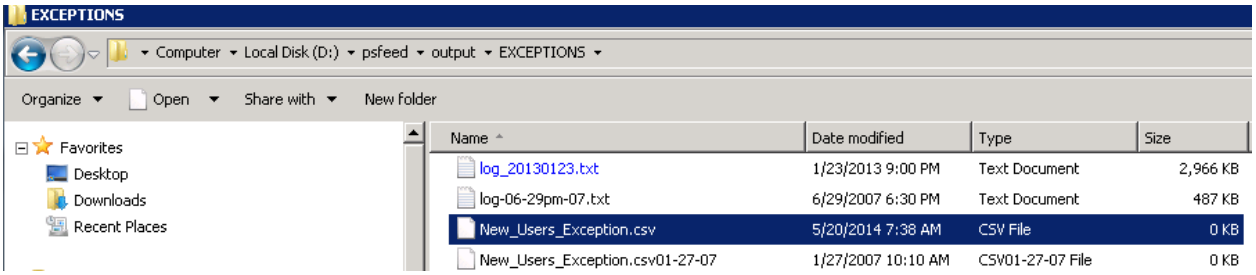


Figura 11: Nuevo Usuario

Ejemplo de récord de un usuario nuevo:

"OscarY","Yos Sanchez,Oscar","Oscar","Yos Sanchez","","114718","01/23/2014","01/01/2015","ITE/ITI","","IDB","","","","","",1,"","MEX","IT Infrastructure","11","","","","","","","Contractor","IDBStdUserADMail_ITE","Y","Y","" "

83

1. Realiza el siguiente análisis de cada récord:

1.1 Asegura que el record tenga un rol

1.2 Revisar si el usuario nuevo existe en Provisioning Manager, Identity Manager y en URA checando por nombre, apellido y username o aliasname, esto es para asegurar que la identidad del usuario es única.

Para records de Staff:

- valida que el record es parte de las notificaciones recibidas por parte de HRD
- Si el usuario existe en PM, IM o URA, revisar si tiene un contrato como Non-Staff

- Si sí, procesa al nuevo usuario como transición de Non-Staff a Staff
- Si no, verificar con recursos humanos porque el usuario está duplicado

Para rcords de non-staff:

- Validar si el record es parte de las notificaciones de los usuario sque pertenecer a agencias o son contratados como terceros
- Si el usuario existe en PM, IM o URA, revisar si tiene un contrato como Staff o como Consultor

- Si sí, procesa al nuevo usuario como transición de Staff a Non-Staff
- Si no, verificar con recursos humanos porque el usuario está duplicado

En caso de que el alias(UserName) en el record es actualmente en uso en PM o URA(aquí el username es equivalente al PCMail ID), un nuevo alias debe ser calculado manualmente por el oficial de seguridad de la información cumpliendo con la lógica standard de creación de una cuenta de AD:

84

Ej. Nombre completo: Peter B. Rabbit:

1. FirstNameLastNameInitial (PETERR)
2. FirstNameInitialLastName (PRABBIT)
3. FirstNameInitialMInitialLastname (PBRABBIT)
4. FirstnameLastnameInitial(2) (PETERRA)
5. FirstnameLastNameInitial(3) (PETERRAB)

Tan pronto como el nuevo UserName/Alias ha sido definido, el record en el correspondiente archivo .csv debería ser actualizado para incluir este valor antes de la ejecución.

1.3 Para el rol missing exception records

Estos casos son generalmente debido a la nueva unidad organizacional agregada o cambiada en el árbol organizacional. Checar en Active Directory y el árbol de People Soft si la unidad ha sido creada

- Si la Org/Unit no exist en Active Directory, verifica si la nueva unidad organizacional tiene una unidad padre creada en el directorio Activo, si sí inserta un nuevo rol asociado a la unidad organizacional padre.

- Si la nueva unidad Organizacional ha sido creada en el árbol de Active Directory, un nuevo rol necesita ser creado en Provisioning Manager.

i. Terminación de usuarios

1. Accesar al servidor *HQPAPROVN* y navegar hacia los directorios *D:\psfeed\output\STAFF*, *D:\psfeed\output\NONSTAFF* y *D:\psfeed\output\EXCEPTIONS*.

2. Copiar la información de los siguientes archivos terminated*_users_role.csv* para Staff, *terminated_users_role_nonstaff.csv* y *terminated_users_faildump.csv* para Non-staff en el correo de PSFEED bajo la sección *TERMINATED_USERS*.

85

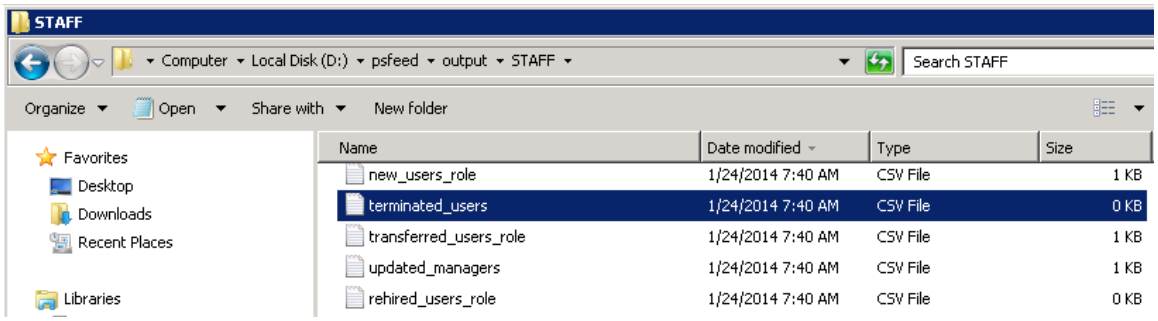


Figura 12: Terminación de Usuario

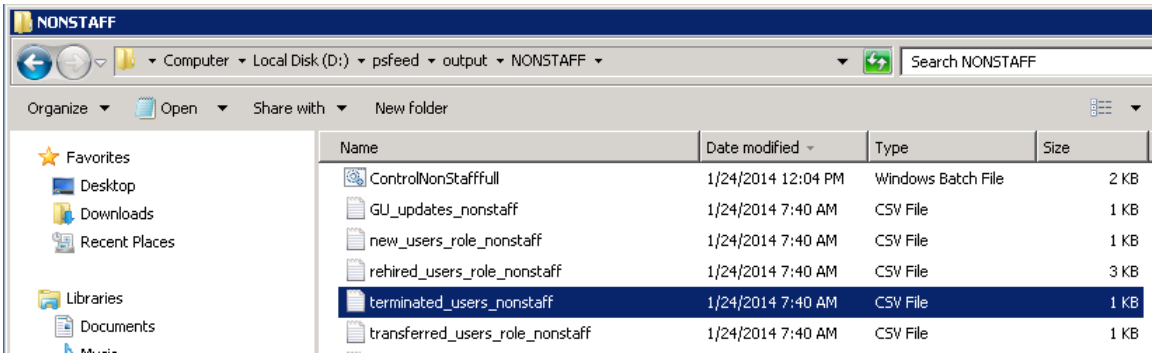


Figura 13: Terminación de Usuario

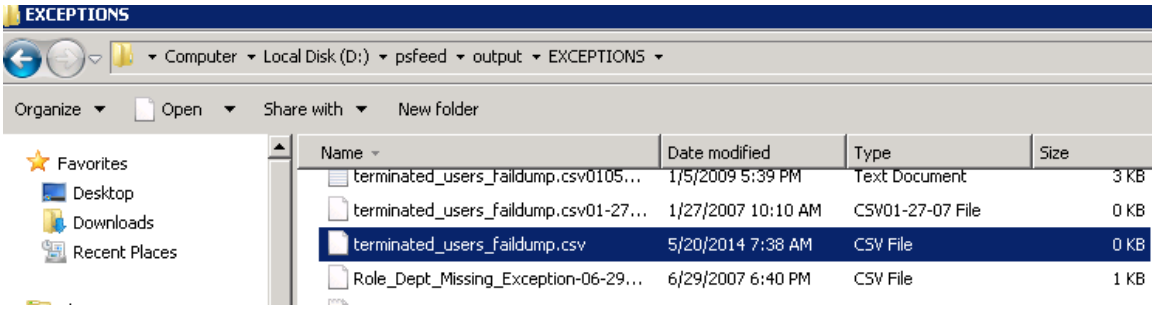


Figura 14: Terminación de Usuario

Ejemplo de record de Terminación:

1,"BRAIANR","Romero Villarreal,Braian","Braian","Romero Villarreal","","114446","09/26/2013","01/24/2014","ITE/ITI","","IDB","","BRAIANR@IADB.ORG","","",0,"","MEX","IT Infrastructure","11","","","","","","","Contractor","Y","Y","","

3. Realizar el siguiente analisis para cada record:

3.1 Verificar que el global user y la cuenta de Active Directory estén activas

Remover cualquier role de terminación de la cuenta global. Este paso es debido a que las cuentas no son borradas en terminación pero son suspendidas guardando el role de IDM en la identidad.

ii. Recontratación de Usuarios

1. Accesar al servidor *HQPAPROVN* y navegar a los directorios *D:\psfeed\output\STAFF*, *D:\psfeed\output\NONSTAFF* y *D:\psfeed\output\EXCEPTIONS*.

2. Copiar la información de los siguientes archivos rehired_*users_role.csv* for Staff, *rehired_users_role_nonstaff.csv* y *rehired_users_role_faildump.csv* para Non-staff en el correo de PSFEED bajo la sección de REHIRED_USERS.

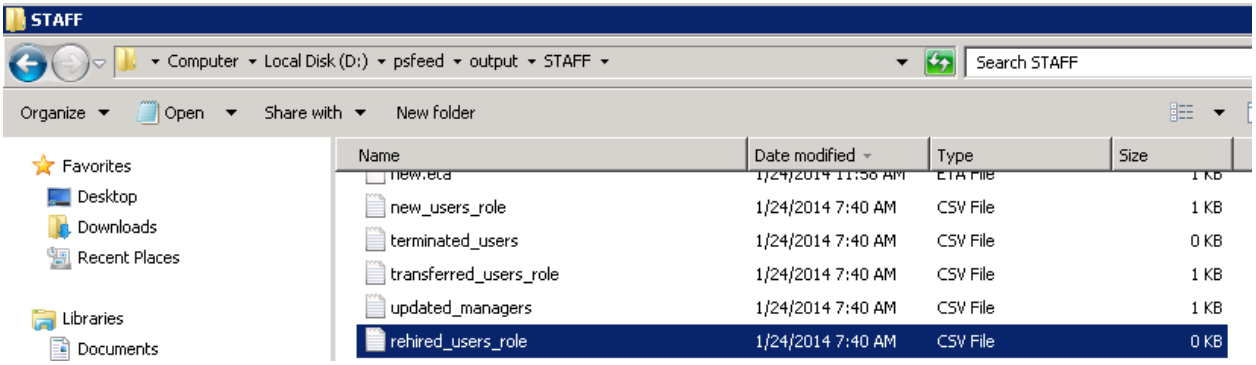


Figura 15: Recontratación de Usuario

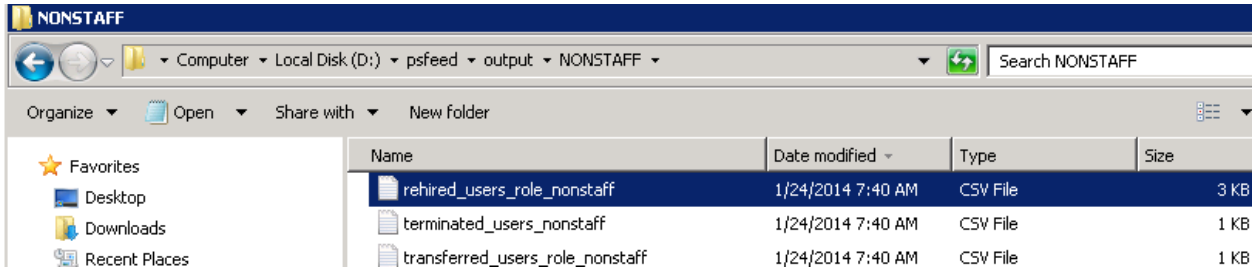


Figura 16: Recontratación de Usuario

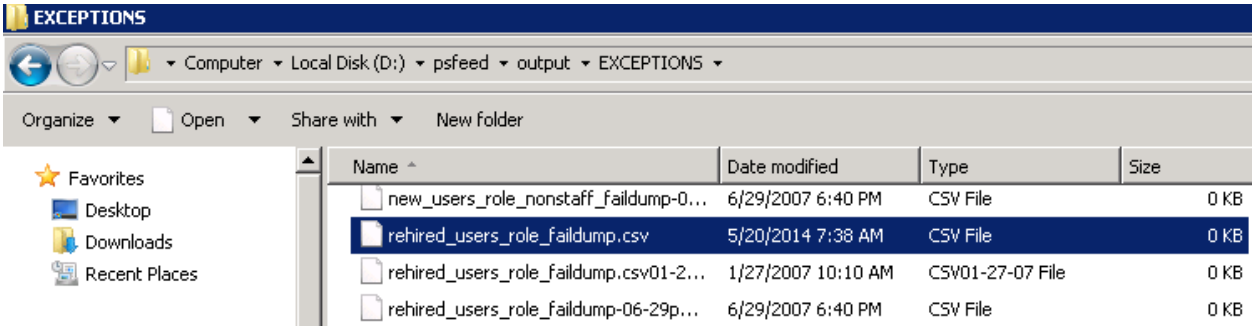


Figura 17: Recontratación de Usuario

87

Ejemplo de un record de recontratación:

2,"HAOD","Deng,Hao","Hao","Deng"," ","114369","01/23/2014","05/01/2014","HRD/ANP"," ","IDB","","HAOD@IADB.ORG"," ","",1," ","HQ","Analytics and Processes Unit","12"," "," "," "," "," ","Contractor","IDBStdUserADMail_HRD","Y","Y"," "

3. Verificar en Provisioning Manager que el Global user este suspendido y tenga el password puesto bajo la pesteña de password, en caso de que el password no este puesto ingresar un nuevo password complejo.

4. Asegurar que la cuenta de AD este deshabilitada en Provisioning Manager.

5. Verificar en Provisioning Manager y en Pro *Prov_File* si la Org/Unit del record recibido es el mismo que el del día anterior. Si este no es igual y el usuario fue terminado antes de 90 días atrás, entonces una transfer tiene que ser aplicada al record inmediatamente después del rehire del usuario.

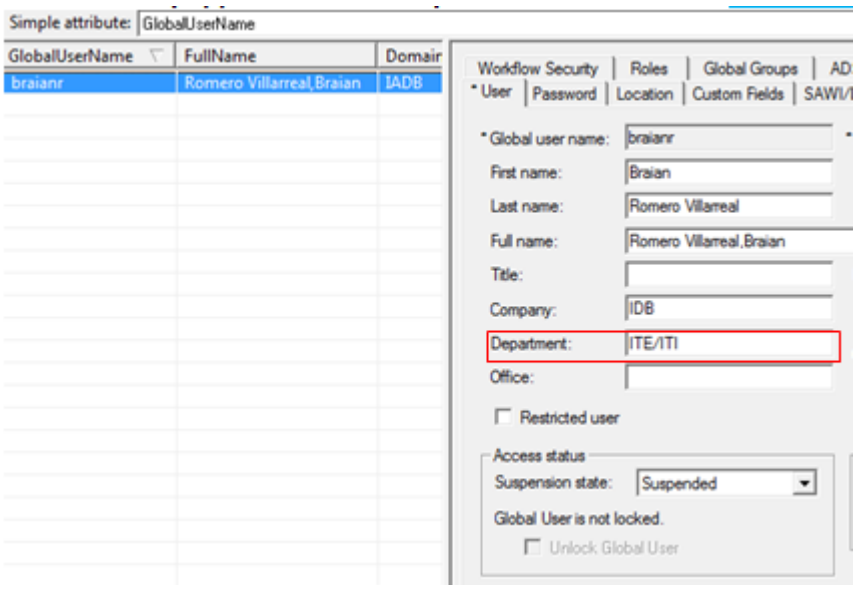


Figura 18: Recontratación de Usuario

6. En Provisioning Manager ir al usuario global del record y en la pestaña de roles mover todos los roles excepto el rol de "*Transfer*".

88

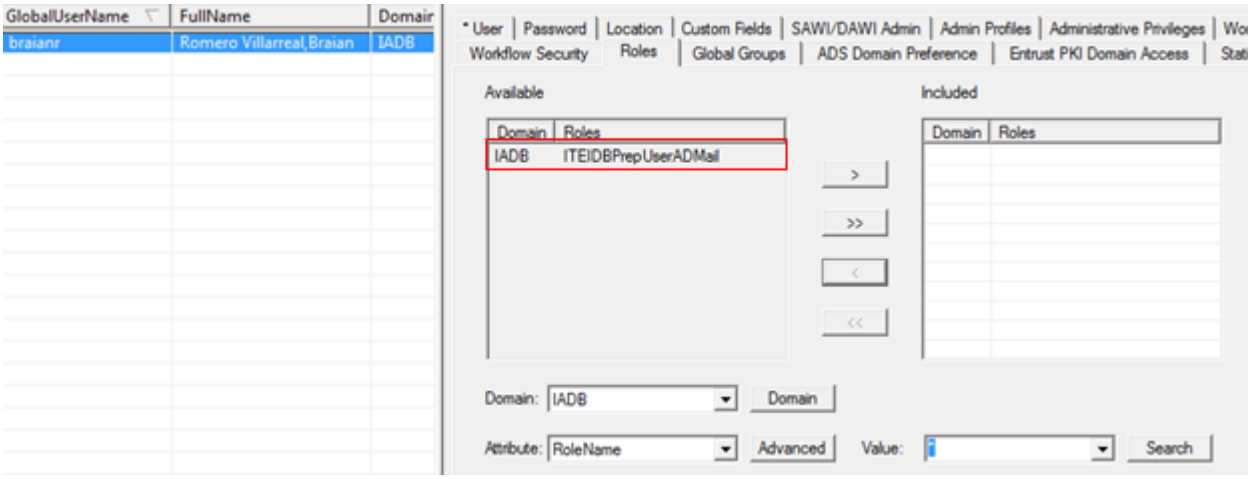


Figura 19: Recontratación de Usuario

7. Verificar en Provisioning Manager que los valores de *Employee ID* y *User Type* son los mismos valores recibidos en los siguientes lugares:

- Usuario Global pestaña "*Custom Fields"*
- Active Directory pestaña "*Custom"*

Actualizar ambos valores antes de procesar el PSFEED

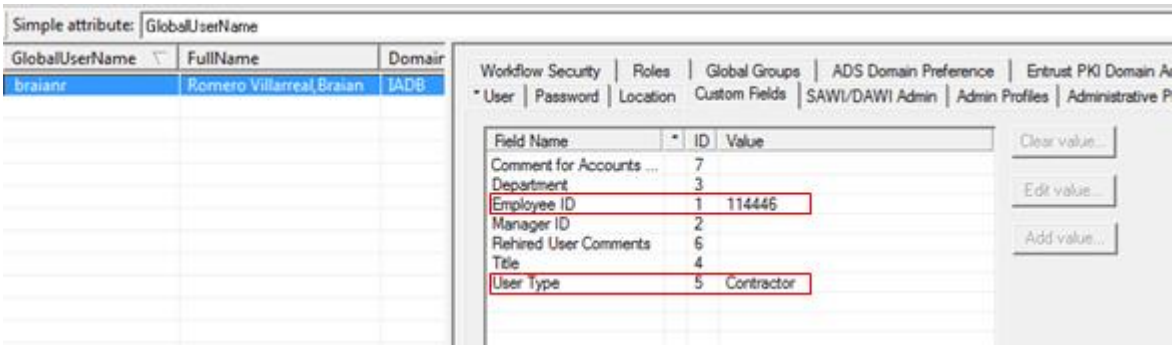


Figura 20: Recontratación de Usuario

8. En provisioning Manager, verificar si el usuario tiene asociadas cuentas de Oracle y/o Unix, estas serán automáticamente reactivadas después de la ejecución.

Si sí, proceder a deshabilitarlas después de que el proceso de recontratación ha sido ejecutado y documentar la acción en el correo de *PSFEED*.

iii. Transferencia de Usuario

89

1. Accesar al server *HQPAPROVN* y navegar en los directorios *D:\psfeed\output\STAFF*, *D:\psfeed\output\NONSTAFF* y *D:\psfeed\output\EXCEPTIONS*.

2. Copiar la información de los siguientes archivos *transferred_users_role.csv* para Staff, *transferred_users_role_nonstaff.csv* y *transferred_users_role_faildump.csv* para Non-staff en el correo de PSFEED bajo la sección de TRANSFERRED_USERS_ROLE.

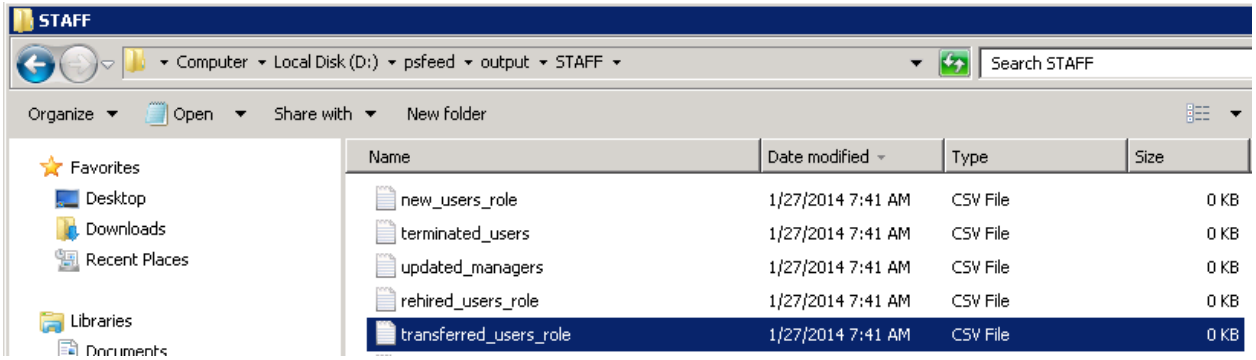


Figura 21:Transferencia de Usuario

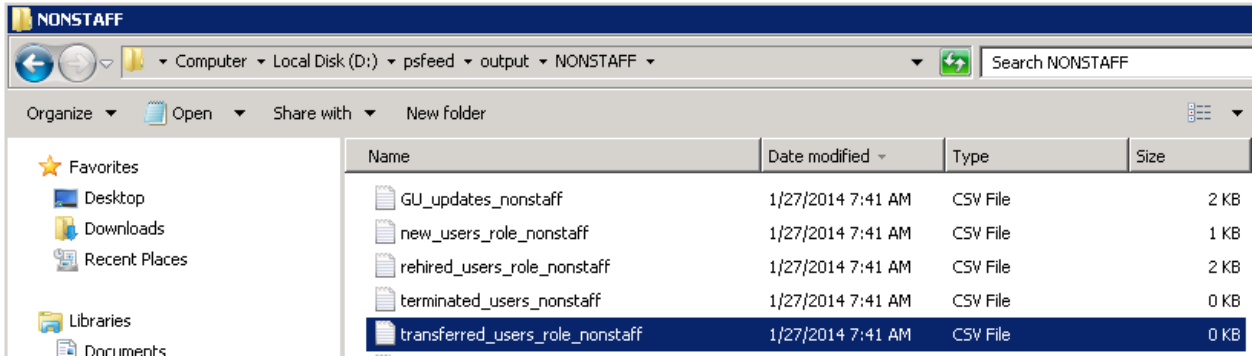


Figura 22:Transferencia de Usuario

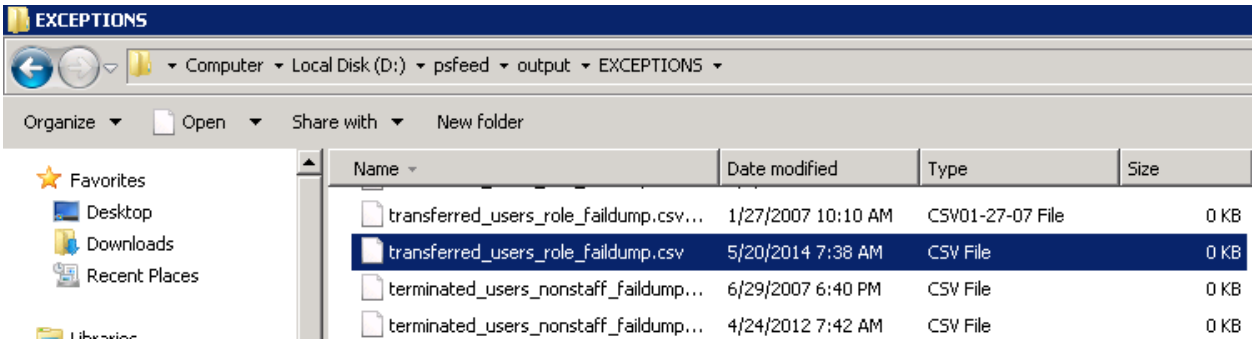


Figura 23:Transferencia de Usuario

Ejemplo de un record de transfer:

1,"MARISOLI","Inurritegui Maurtua,Marisol","Marisol","Inurritegui Maurtua"," ","112879","01/16/2012","","RND/CEC"," ","IDB","225-7950","MARISOLI@IADB.ORG","104042","HECTORMAL",1," ","ECU","Rural Dev and Nat Dis - CEC"," 0"," "," "," "," "," ","Staff","RND/CGY"," ","CEC_Transfer_UPO","Y","Y"," "

3. Verificar en Provisioning Manager que las cuentas de Global User y el Active Directory estén activas y puestas como never expire

4. Verificar en Provisioning Manager que los Valores de *Employee ID* y *User Type* son los mismos valores recibidos en los siguientes lugares:

- Usuario Global pestaña "*Custom Fields"*
- Active Directory pestaña "*Custom"*

Actualizar ambos valores antes de procesar el PSFEED

5. Checar en Provisioning Manager que el Global User tenga puesto un password bajo la pestaña de Password, en caso de no tener un password puesto, ingresar un nuevo password complejo.

iv. Actualizacion de Usuario Global

1. Este Evento actualiza el manager del usuario

2. Accesar el servidor *HQPAPROVN* y navegar a los directorios *D:\psfeed\output\STAFF* y *D:\psfeed\output\NONSTAFF*.

3. Copiar la información de los siguientes archivos updated_managers*.csv* para Staff y GU_updates *_nonstaff.csv* para Non-staff en el correo de PSFEED bajo las secciones de *UPDATED_MANAGERS* o *GU_UPDATED_NONSTAFF*

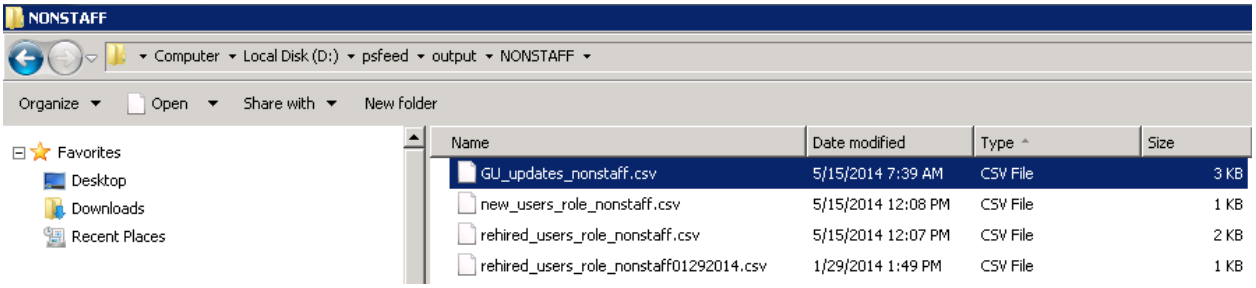


Figura 24 actualización de fecha de contrato del Usuario

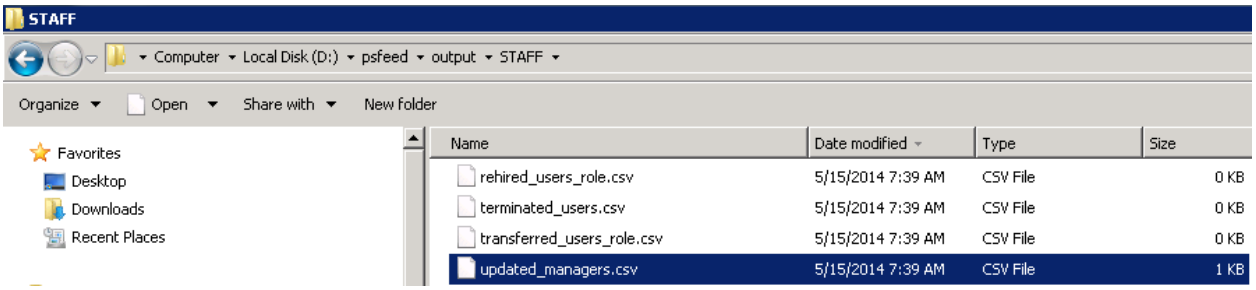


Figura 25 actualización del jefe del Usuario

4. Verificar en Provisioning Manager que la cuenta de Active Directory del usuario este puesta como Never expire.

Procesar

Una vez que los records han sido revisados e identificadas las acciones y documentadas, los pasos para procesar son los siguientes.

1. Para todos los archivos .csv que necesitan ser actualizados con la información de la revisión, crear un respaldo del archivo original

2. Editar los archivos originales .csv con la información actualizada pues estos son los que se ejecutaran.

3. Editar el archivo .bat para ejecutar los eventos de provisioning con las acciones actualizadas en los archivos .csv, para dejar fuera un evento del archivo .bat se antepone las siglas REM(remove) para omitir su ejecución.

Para Staff el archivo .bat se llama *ControlSTAFFpartial.bat*

92

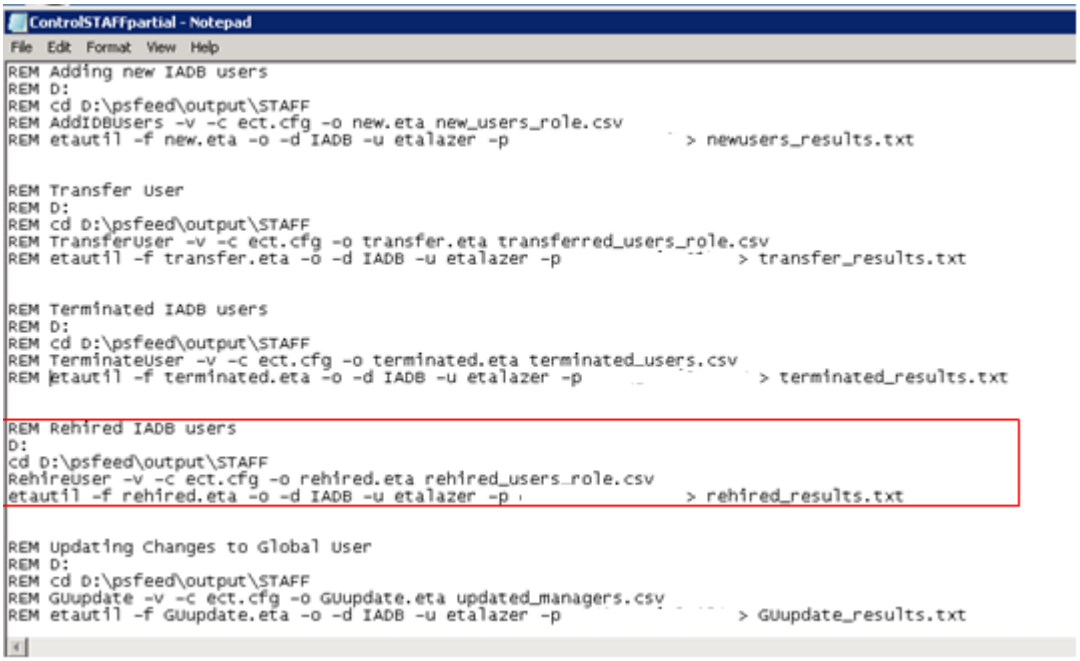


Figura 26 Procesar psfeed

Para Staff el archivo .bat se llama *ControlSTAFFpartial.bat*

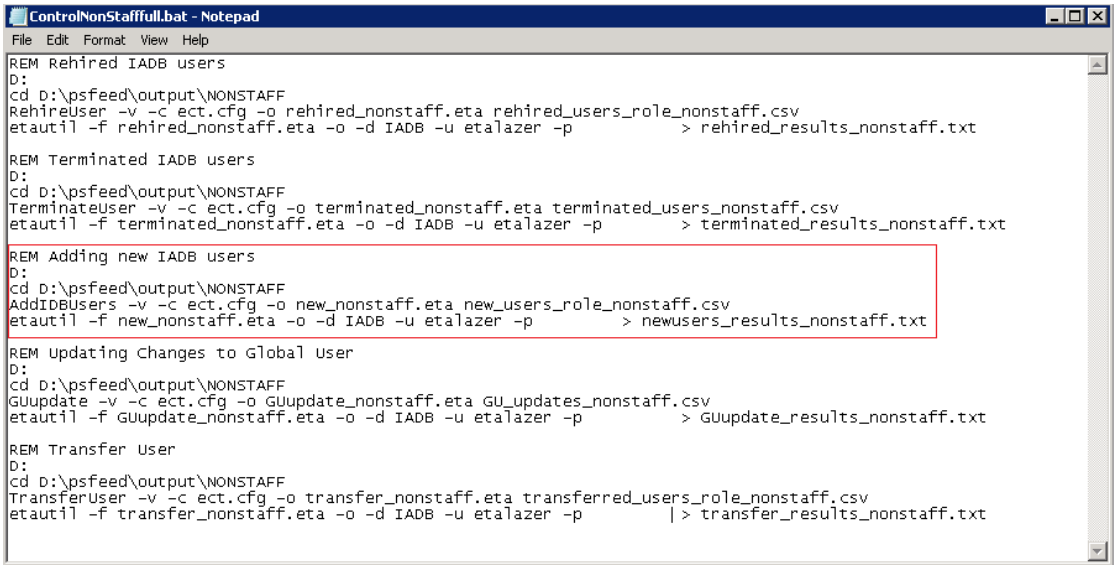


Figura 27 Procesar psfeed

La ejecución de los archivos .bat corren ejecutables de C# que convierten los records de los usuarios con la información de los archivos .csv arriba mencionados en el formato de la herramienta CA. La herramienta de CA es ejecutada para procesar los eventos de provisioning, la ejecución produce un archivo de resultados para cada evento.

93

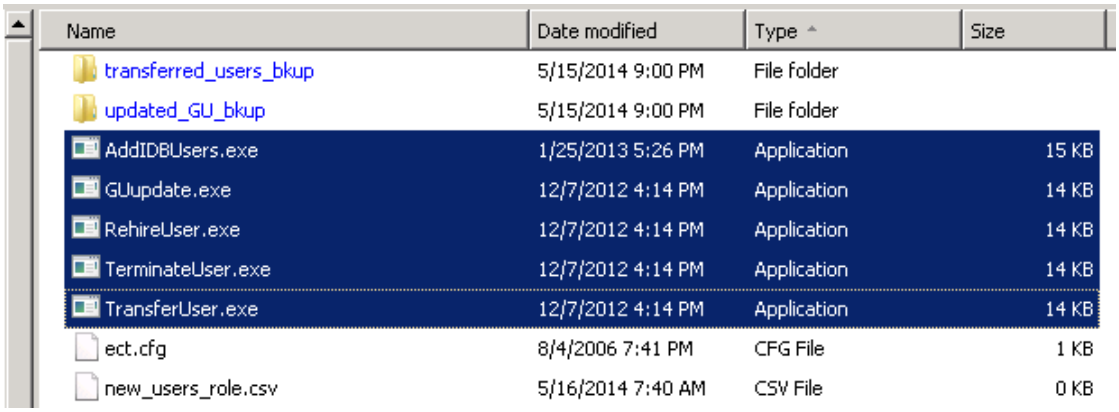


Figura 28 ejecución del los archivos .exe

b. Verificación

La ejecución genera un archivo de resultados para cada eventoen los correspondientes folders *D:\psfeed\output\STAFF* y *D:\psfeed\output\NONSTAFF*. Cada archivo necesita ser revisado y analizado para checar posibles errores. En caso de encontrar un error, se realizará un análisis para encontrar la causa raíz.

NOTA: *Un error común es "Timeout"*, cuando aparece este error es debido a la latencia del sistema y solo los records que fallaron se tienen que reprocesar.

i. Nuevo Usuario

1. Verificar que las notificaciones de correo electrónico de los eventos salieron

Si la cuenta esta bajo el dominio de IDB (HQ) un correo de notificación de eTrsut Admin es enviada a Service Desk *ITE Client Center (ICC)* HELPDESK@iadb.org; *Information Security* sqainfosec@iadb.org; eMail Group EMAILGROUP@iadb.org como recipientes bases y actores para otras tareas de provisioning.

Si la cuenta es bajo el dominio de REG (Country Offices), las notificaciones son dirigidas al equipo de soporte de IT de cada país, por ejemplo CXXTechSup@iadb.org, (donde XX representa el pais), *Information Security* sqainfosec@iadb.org, y eMail Group EMAILGROUP@iadb.org.

2. Verificar en Provisioning Manager que las cuentas de Global user y Active Directory fueron creadas y están habilitadas.

3. Checar que la unidad Organizacional del contenedor en Active Directory donde las cuentas son creadas coincide con el Org/Unit del record del usuario.

94

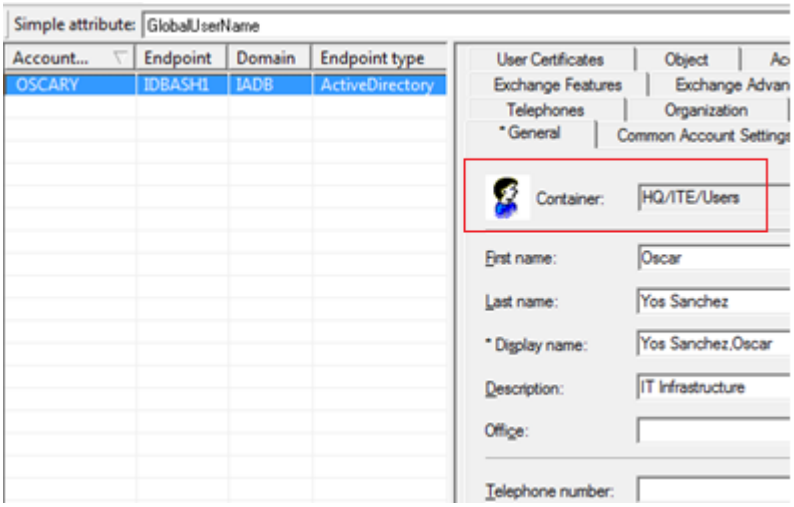


Figura 29 Nuevo Usuario

ii. Terminacion de usuario

1. Verificar que las notificaciones de correo electrónico de los eventos salgan a sus recipientes destinatarios.

Para terminación de usuarios, las notificaciones se deben enviar a otros equipos para sus acciones: CXXTechSup@iadb.org, sqainfosec@iadb.org, EMAILGROUP@iadb.org, ITECOMPLIANCE@iadb.org, remedysupport@iadb.org, ITSecurity-INFRA@iadb.org.

2. Verificar en Provisioning Manager que las cuentas, usuario global está suspendido y las cuentas correlacionadas están deshabilitadas.

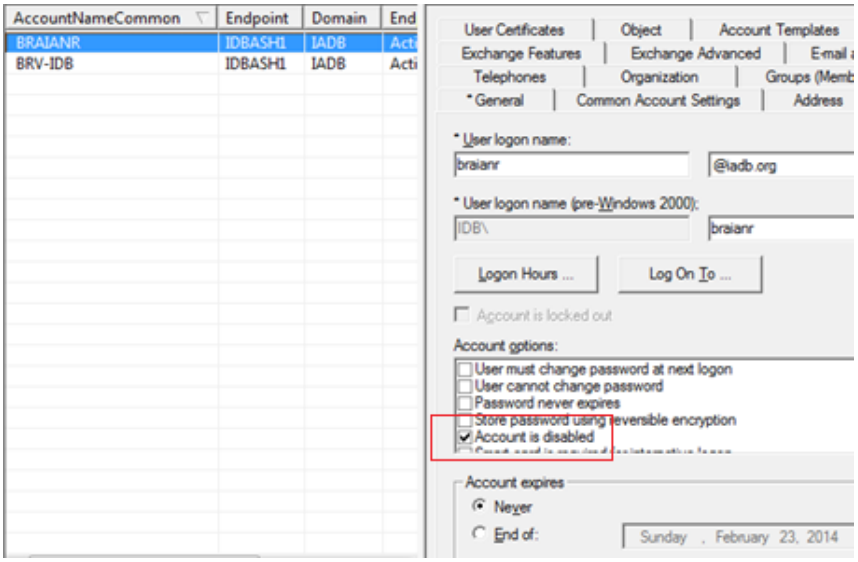


Figura 30 Terminación de Usuario

95

Una vez que la cuenta está suspendida, un script desconecta el buzón de correo electronico de la cuenta de AD cuando está en la unidad ToBeDeleted el mismo día que la cuenta es deshabilitada. Este script está programado para correr cada 12 horas para asegurar el proceso. Después de que la cuenta está deshabilitada por 90 días la cuenta se borra de AD.

iii. Recontratación de usuarios

1. Verificar que las notificaciones de correo electrónico de los eventos de recontratación salieron a sus recipientes destinatarios.

- Si la cuenta está bajo el dominio IDB(HQ) un correo electronico de notificación de *eTrust Admin* etraustadmin@iadb.org es enviado a *ITE Client Center (ICC)* Helpdesk@iadb.org, *Information Security* sqainfosec@iadb.org, *eMail Group* EMAILGROUP@iadb.org.

- Si la cuenta está bajo el dominio de REG(Country Offices) un correo de notificación de *eTrust Admin* etrustadmin@iadb.org es enviado al soporte local del país correspondiente CXXTechSup@iadb.org, *Information Security* sqainfosec@iadb.org, y *eMail Group* EMAILGROUP@iadb.org

2. Si el usuario ha sido recontratado/reactivado pero el buzón de correo electrónico está desconectado de la cuenta de AD, el proceso de reactivación reconecta o crea un buzón de correo nuevo.

3. Si el usuario está siendo recontratado en una Org/Unit diferente, una transferencia manual se tiene que aplicar después del proceso de recontratación.

iv. Transferencia de Usuarios

1. Verificar que las notificaciones de correo electrónico de los eventos de Transferencia salieron a sus recipientes destinatarios.

- Si la cuneta está bajo el dominio IDB(HQ) una notificación de correo electrónico de *eTrust Admin* etraustadmin@iadb.org es enviada a *ITE Client Center (ICC)* Helpdesk@iadb.org, *Information Security* sqainfosec@iadb.org, *eMail Group* EMAILGROUP@iadb.org, y *GRC group* ITECOMPLIANCE@iadb.org.

96

- Si la cuenta está bajo el dominio REG(Country Offices) una notificación de correo electrónico de *eTrust Admin* etrustadmin@iadb.org es enviado al equipo de tecnología local del correspondiente pais CXXTechSup@iadb.org, *Information Security* sqainfosec@iadb.org, *eMail Group* EMAILGROUP@iadb.org, y *GRC group* ITECOMPLIANCE@iadb.org.

2. Si el usuario es movido a una diferente Org/Unit en el mismo dominio, el servicio de correo electrónico no es interrumpido. Un script mueve la cuenta de AD a su correspondiente unidad en el dominio de Active Directory

3. Si el usuario se mueve a diferente Org/Unit en el mismo dominio, la conectividad del correo electrónico no es interrumpido, un script mueve la cuenta a la correspondiente Org Unit.

4. Si el usuario se mueve entre dominios, se necesita una coordinación entre el equipo de IT local del país, el equipo de Active Directory e Information Security, de tal manera que la cuenta del usuario(AD y mailbox) sea movida a su unidad correspondiente en AD

Actualización de usuario Global

Para verificar la actualización del usuario global, verificar que la actualización del ID del manager y el fin del contrato son reflejados wn el record del usuario.

Transferecnia Manual

Una transferencia manual es necesaria cuando la recontratación del usuario es en una Org/Unit diferente que la que tenia en su ultima terminacióny la terminación no ha pasado más de 90 días. Si los accesos han sido removidos la transferencia manual no es necesaria.

v. Cambio de banderas de provisioning

Los cambios de banderas son entrados por los oficiales de contratos en People Soft, esto genera una notificación de correo electrónico recibida en el buzon departamental de seguridad de la información.

vi. 5 dias de gracia

Un caso excepcional, la extensión de contrato de los usuarios o renovación que son retrasados, cuando esto sucede, el oficial de contratos solicita a el equipo de segudad de la información mantener la cuenta de algún usuario activa o reactivarla en caso de que haya sido suspendida. Para proceder

97

con la reactivación se necesita aprobación del Manager de el departamento de Seguridad de la información.

1 Requerir evidencia mostrando que el contrato ha sido ingresado en People Soft y ha sido aprobado, las banderas de provisioning deben estar en YY.

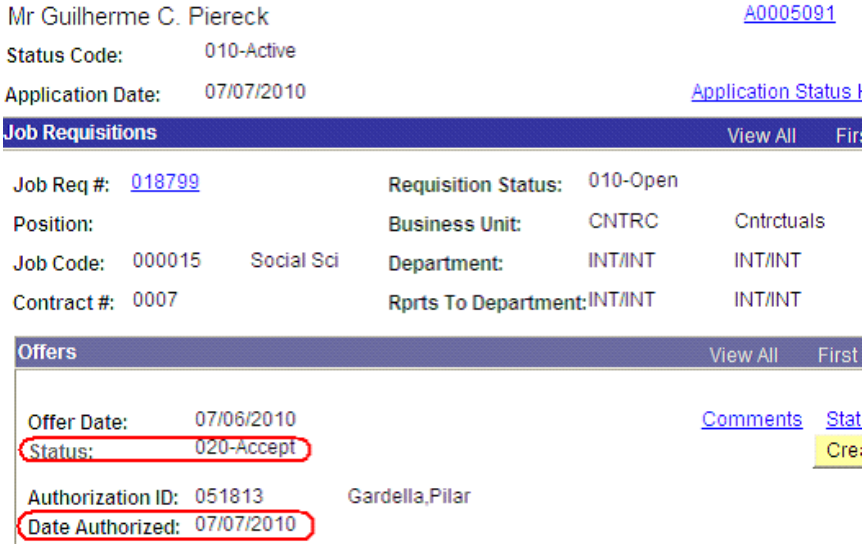


Figura 31 Días de gracias

2 Otorgar cinco días calendario de gracia haciendo los siguientes pasos:

- Checar que en Provisioning Manager el usuario este suspendido

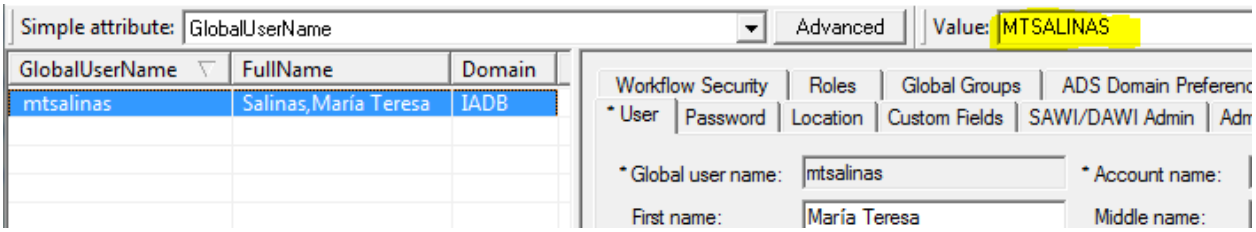


Figura 32 Días de gracias

98

- Dar click derecho en el usuario y seleccionar listar cuentas

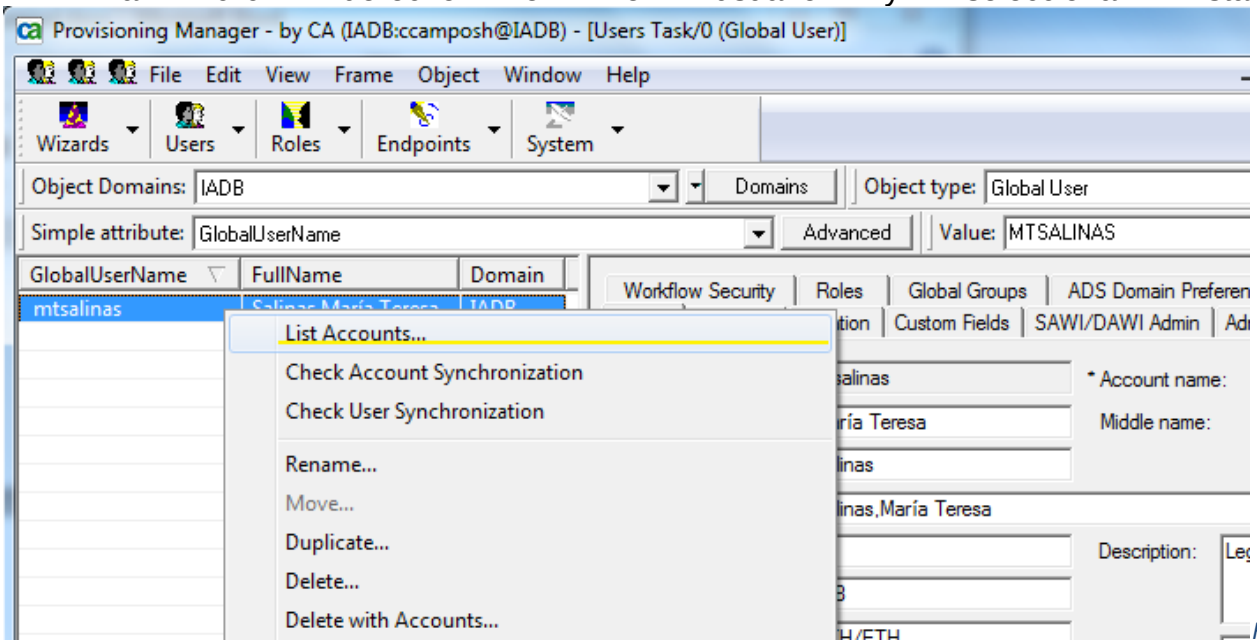


Figura 33 Días de gracias

- Doble click en la cuenta de Active Directory

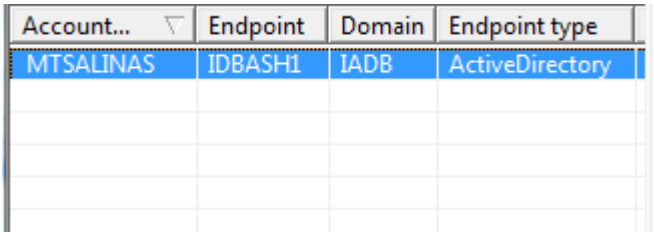


Figura 34 Días de gracias

- Ir a la pestaña *Account

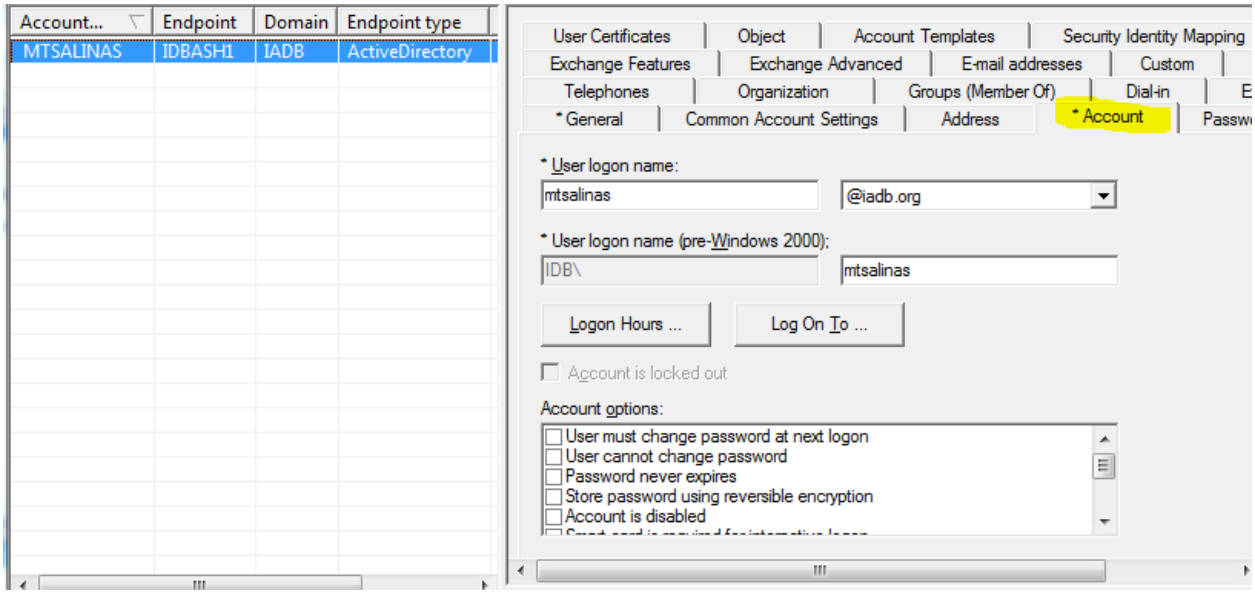


Figura 35 Días de gracias

- En el Account options, seleccionar la opción End of seleccionando los cinco días de gracia apartir de la fecha actual

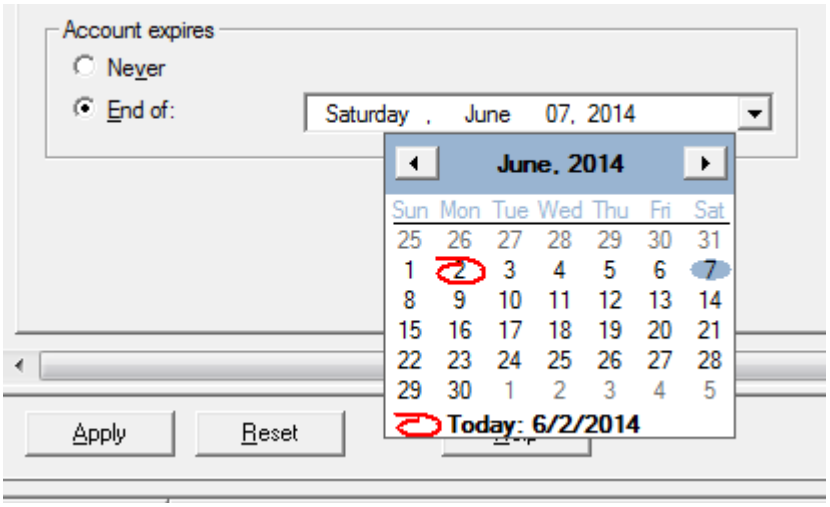


Figura 36 Días de gracias

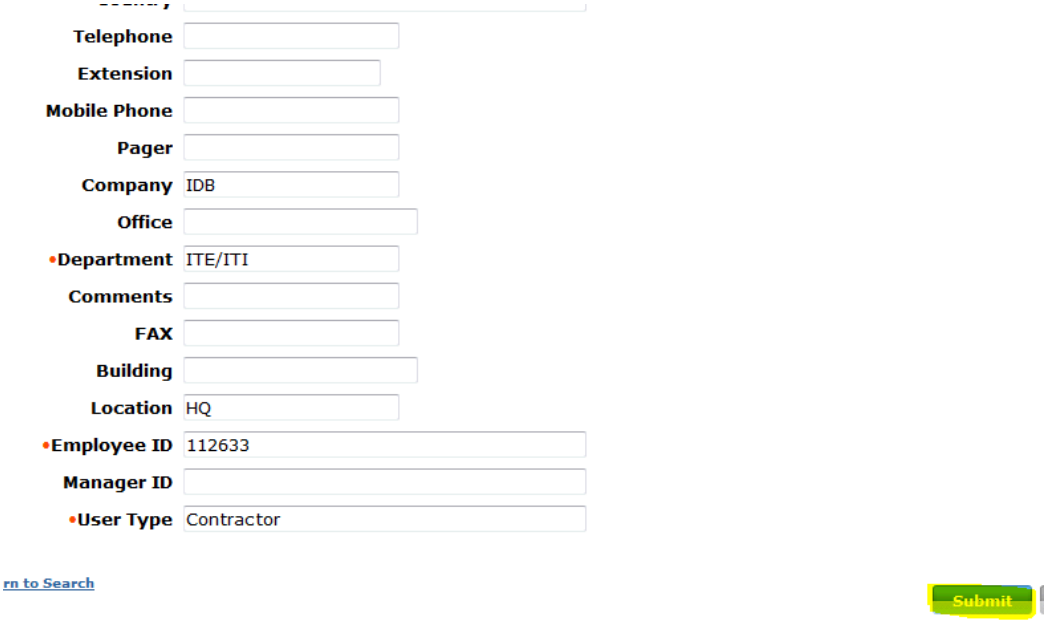


Figura 37 Días de gracias

El record del usuario deberá llegar en el PSFEED con la nueva fecha del contrato, cuando este record llegue el oficial de seguridad deberá poner la cuenta como never expire.

1.14 Paquete SSIS

El paquete SSIS es el artefacto que provee al equipo de Seguridad de la Información con los records que fueron modificados en la plataforma de recursos humanos People Soft.

Este paquete se ejecuta todos los días a las 6 am.

Si el paquete falla se le pide al equipo de DBA que se ejecute nuevamente el paquete SSIS

Reconciliación de cuentas entre PeopleSoft y Active Directory

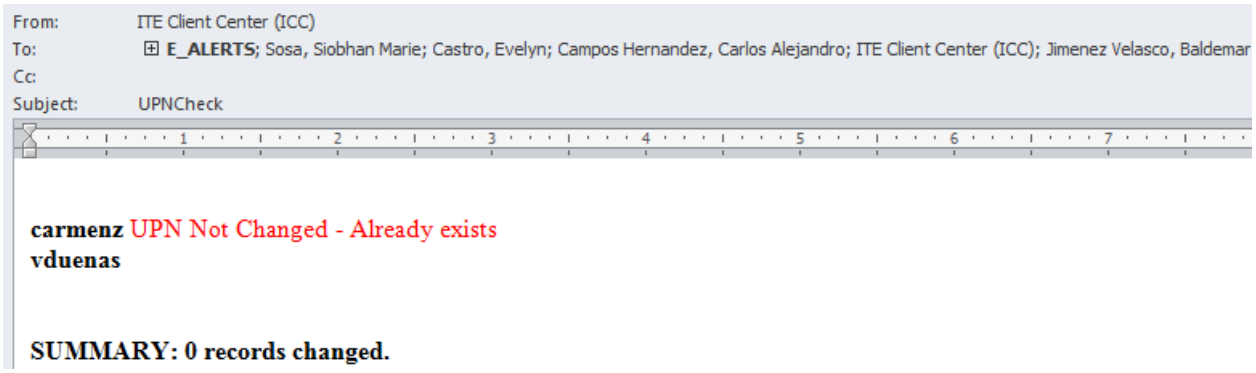
Proposito

Para reconciliar el archivo de provisioning de People Soft de records activos contra la lista de cuentas activas de Active Directory en todos los dominios IDB, REG. Este proceso se ejecuta cada dos semanas.

1.15 Alertas de cuentas duplicadas

Las notifcaciones de email son recibidas en el buzon de INFOSEC al sgainfosec@iadb.org indicando el estatus de las cuentas recién creadas.

101



Cuando existe un record en rojo indicando que la cuenta existe, esto significa que la cuenta de AD especifica está duplicada. La cuenta nueva(duplicada se tiene que borrar y calcular un nuevo alias)

Al siguiente día la cuenta ya no debe aparecer en rojo.

102

Eventos procesados en el sistema de provisionamiento

En las tablas de abajo se muestran los eventos procesados en el sistema de provisionamiento durante los años 2012, 2013, 2014 Y 2015

Los eventos procesados son Transferencia, Nuevo usuario, recontratación y terminaciones

Tabla 46

2012	Transferencia	Nuevo usuario	Recontratación	Terminación
ENERO	83	111	28	145
FEBRERO	61	98	37	42
MARZO	45	114	115	138
ABRIL	56	84	93	152
MAYO	56	107	92	156
JUNIO	43	149	81	115
JULIO	64	142	108	198
AGOSTO	46	129	107	203
SEPTIEMBRE	50	84	93	178
OCTUBRE	47	122	54	135
NOVIEMBRE	44	90	79	100
DICIEMBRE	27	76	48	135
TOTAL	622	1306	935	1697
PROMEDIO	51.83333333	108.8333333	77.91666667	141.4166667

103

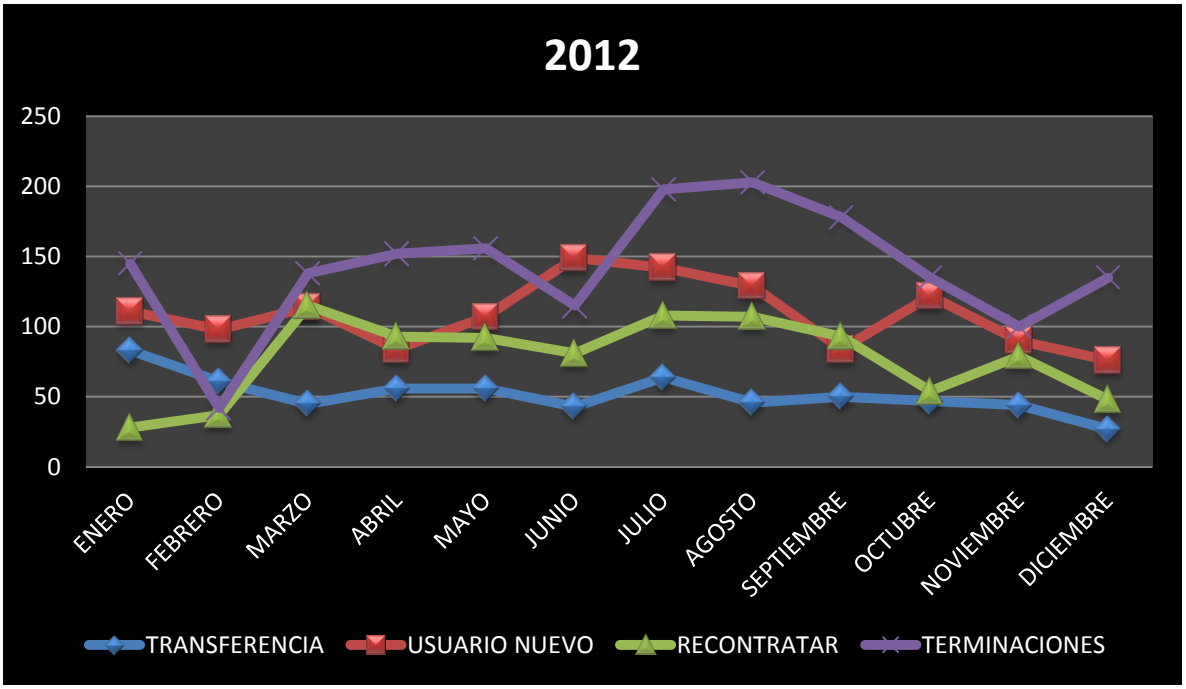


Tabla 47

2013	Transferencia	Nuevo usuario	Recontratación	Terminación
ENERO	107	134	124	319
FEBRERO	61	77	84	107
MARZO	62	86	83	133
ABRIL	74	100	75	167
MAYO	74	162	81	128
JUNIO	38	160	74	103
JULIO	50	136	89	171
AGOSTO	50	119	75	204
SEPTIEMBRE	59	126	68	158
OCTUBRE	52	112	71	118
NOVIEMBRE	30	74	52	72
DICIEMBRE	32	83	48	128
TOTAL	689	1369	924	1808
PROMEDIO	57.41666667	114.0833333	77	150.6666667

104

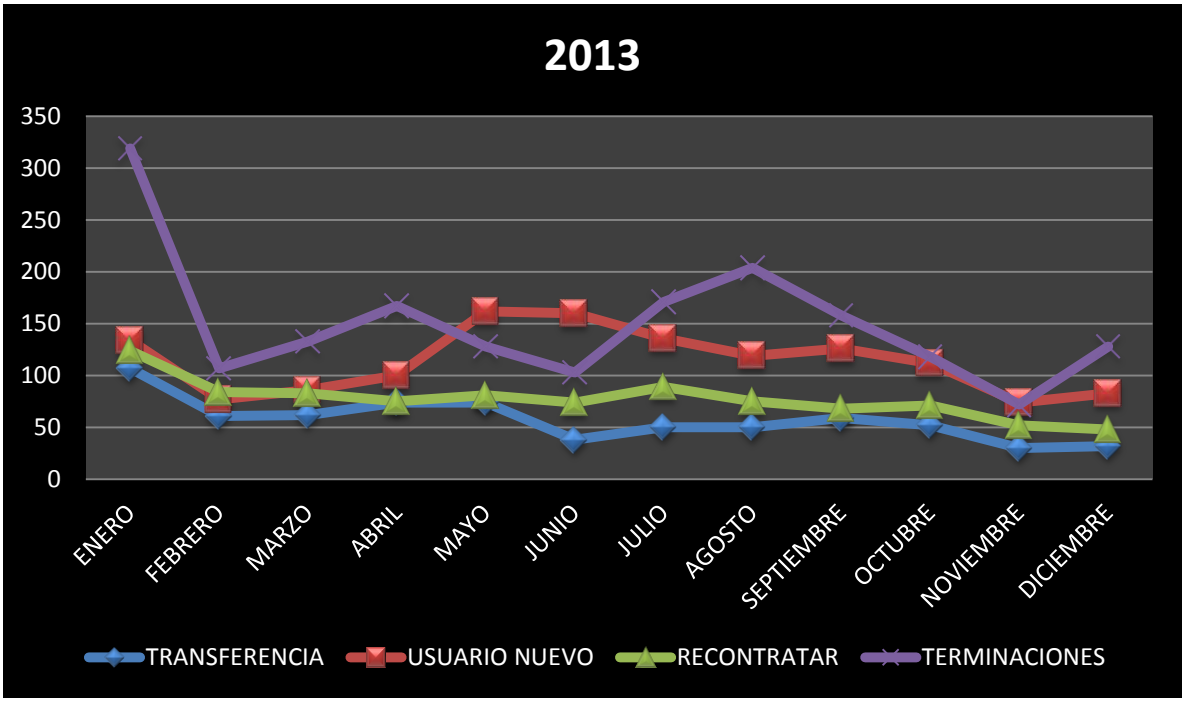


Tabla 48

2014	Transferencia	Nuevo usuario	Recontratación	Terminación
ENERO	132	135	108	294
FEBRERO	75	92	84	82
MARZO	110	91	58	120
ABRIL	90	96	65	124
MAYO	55	113	43	91
JUNIO	47	193	71	150
JULIO	66	160	73	232
AGOSTO	38	160	64	95
SEPTIEMBRE	41	104	69	92
OCTUBRE	58	111	81	167
NOVIEMBRE	34	85	56	94
DICIEMBRE	42	85	47	143
TOTAL	788	1425	819	1684
PROMEDIO	65.66666667	118.75	68.25	140.3333333

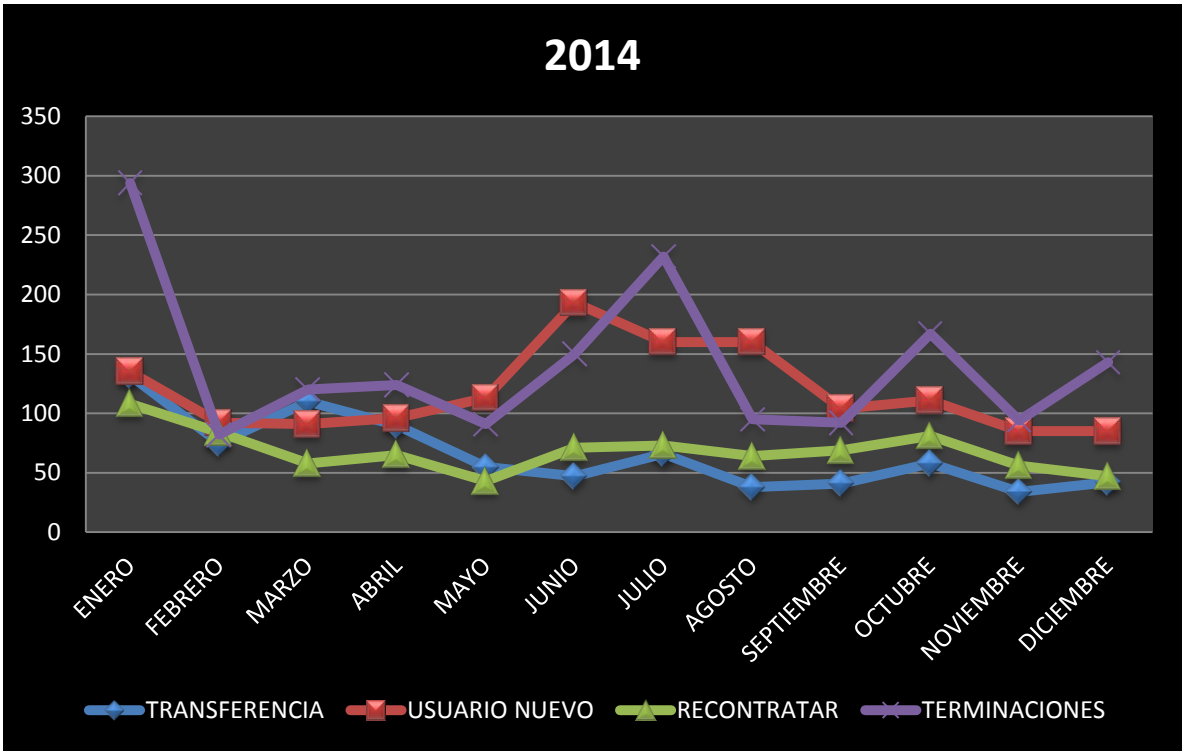


Tabla 49

2015	Transferencia	Nuevo usuario	Recontratación	Terminación
ENERO	67	92	30	145
FEBRERO	30	117	65	97
MARZO	59	108	94	143
ABRIL	41	72	60	187
MAYO	33	98	55	115
JUNIO	48	141	61	126
JULIO	52	134	58	147
AGOSTO	51	106	51	171
SEPTIEMBRE	37	96	63	152
OCTUBRE	33	111	83	182
NOVIEMBRE	65	83	59	135
DICIEMBRE	186	85	65	167
TOTAL	702	1243	744	1767

106

PROMEDIO	58.50	103.58	62.00	147.25

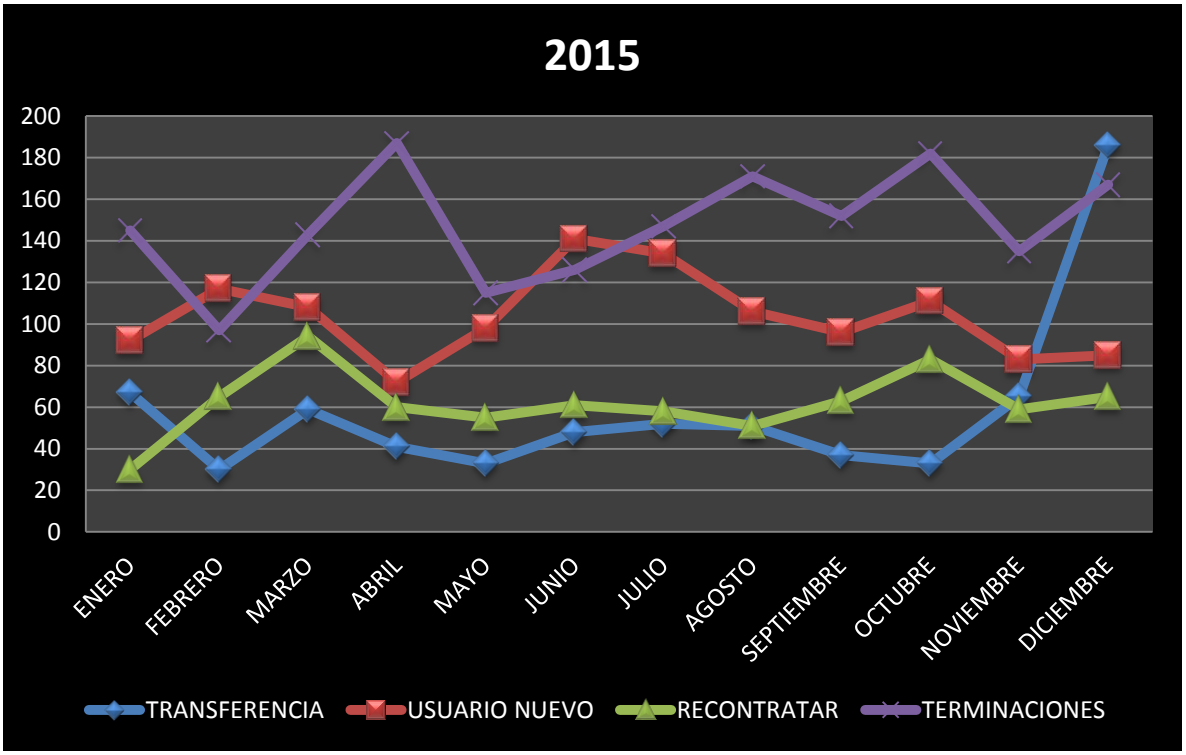
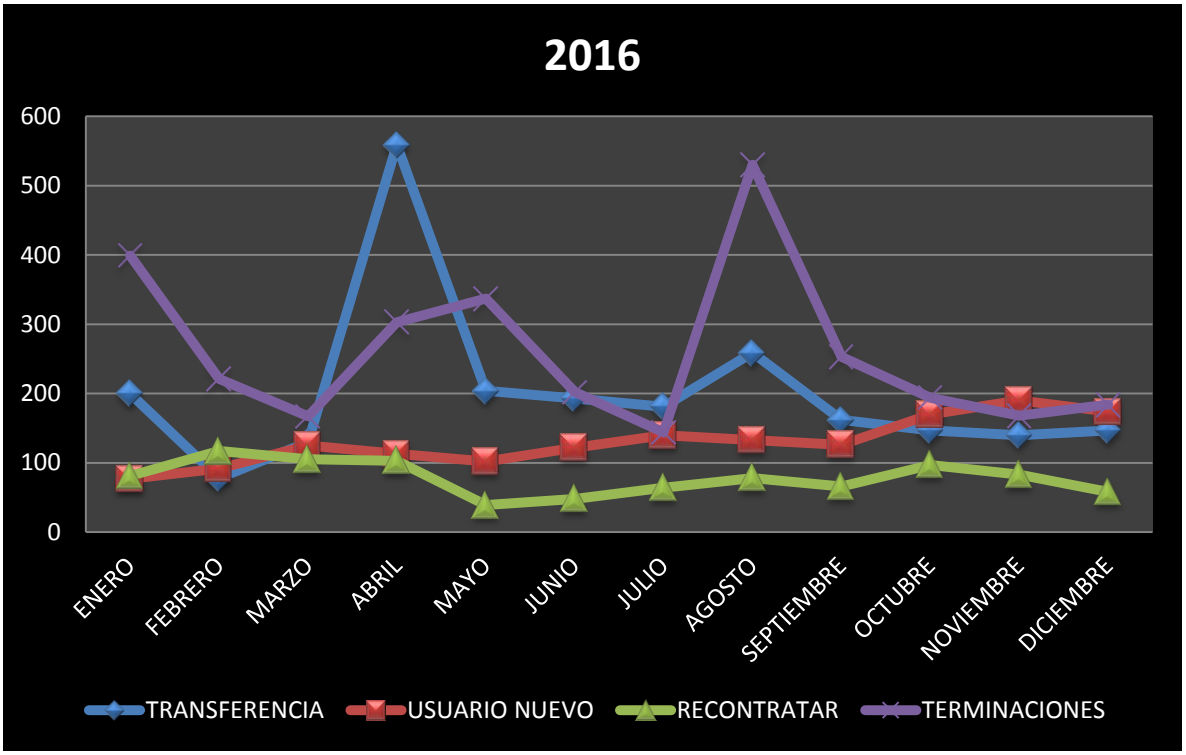


Tabla 50

2016	Transferencia	Nuevo Usuario	Recintrataciones	Terminaciones
ENERO	200	77	81	399
FEBRERO	78	92	117	221
MARZO	130	125	105	167
ABRIL	559	113	103	303
MAYO	204	102	39	337
JUNIO	193	122	48	202
JULIO	181	140	64	144
AGOSTO	259	133	78	530
SEPTIEMBRE	162	126	66	253
OCTUBRE	147	170	97	194
NOVIEMBRE	140	190	83	168
DICIEMBRE	147	174	58	184
TOTAL	2400	1564	939	3102
PROMEDIO	200.00	130.33	78.25	258.50

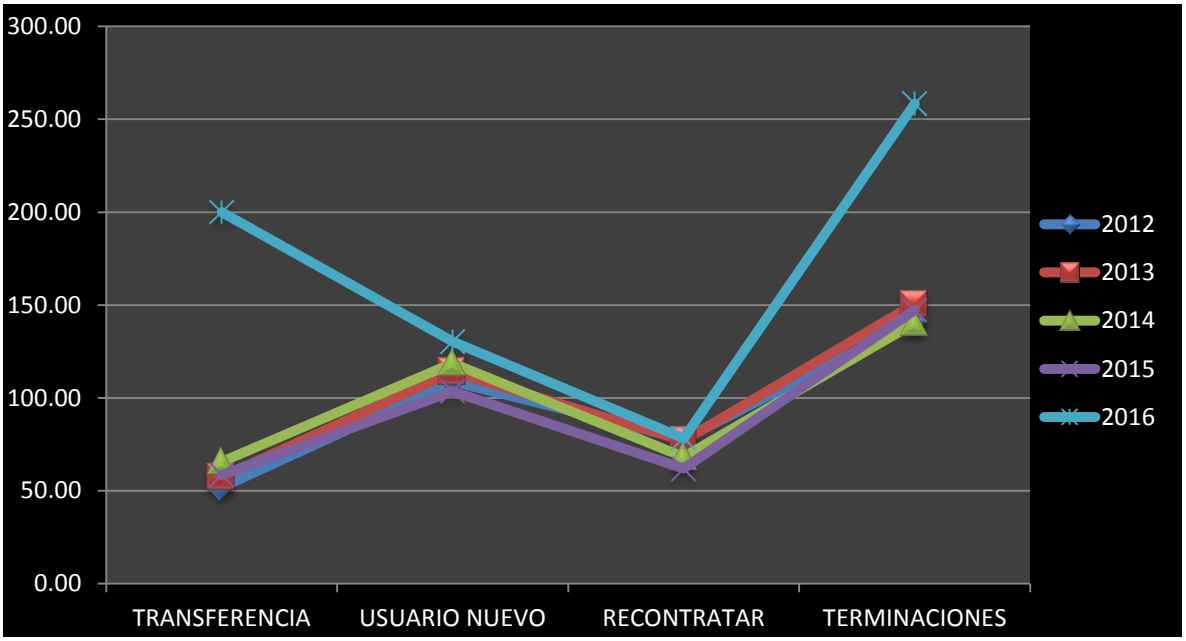
107



Promedios

	2012	2013	2014	2015	2016
TRANSFERENCIA	51.83	57.42	65.67	58.50	200.00
USUARIO NUEVO	108.83	114.08	118.75	103.58	130.33
RECONTRATAR	77.92	77.00	68.25	62.00	78.25
TERMINACIONES	141.42	150.67	140.33	147.25	258.50

108



Mapas de AD

Cuando las cuentas de Active Directory son creadas por el proceso de provisioning se crean en su respectiva unidad organizacional, por ejemplo si el usuario pertenece a la unidad de ITE, la cuenta de Active Directory es creada en el dominio IDB dentro de la unidad ITE. Cada carpeta en el Active Directory correspondiente a una Unidad Organizacional tiene grupos, memebresias y políticas que aplican directamente a la cuenta del usuario una vez que esta dentro su Org Unit.

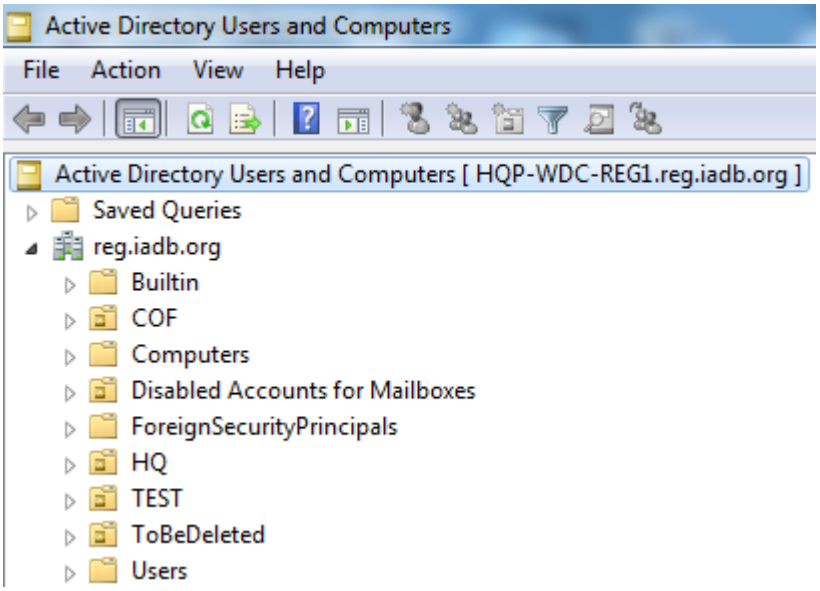


Figura 38 Mapas de AD

109

Organización en Active Directory del Dominio IDB de los head quarters del Banco Inter Americano de Desarrollo

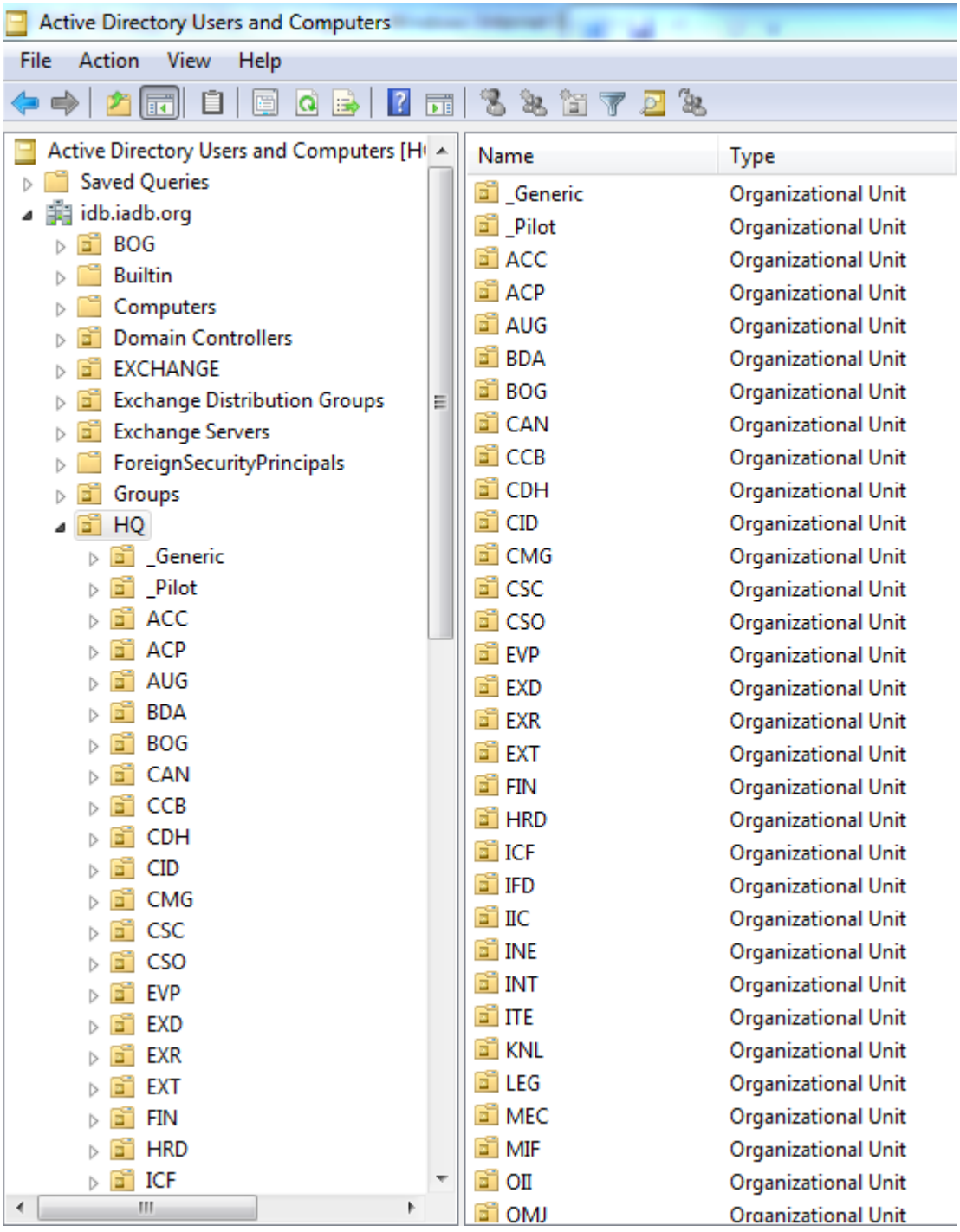


Figura 39 Mapas de AD

Organización en Active Directory del Dominio REG de los Country Offices(COF) del Banco Inter Americano de Desarrollo

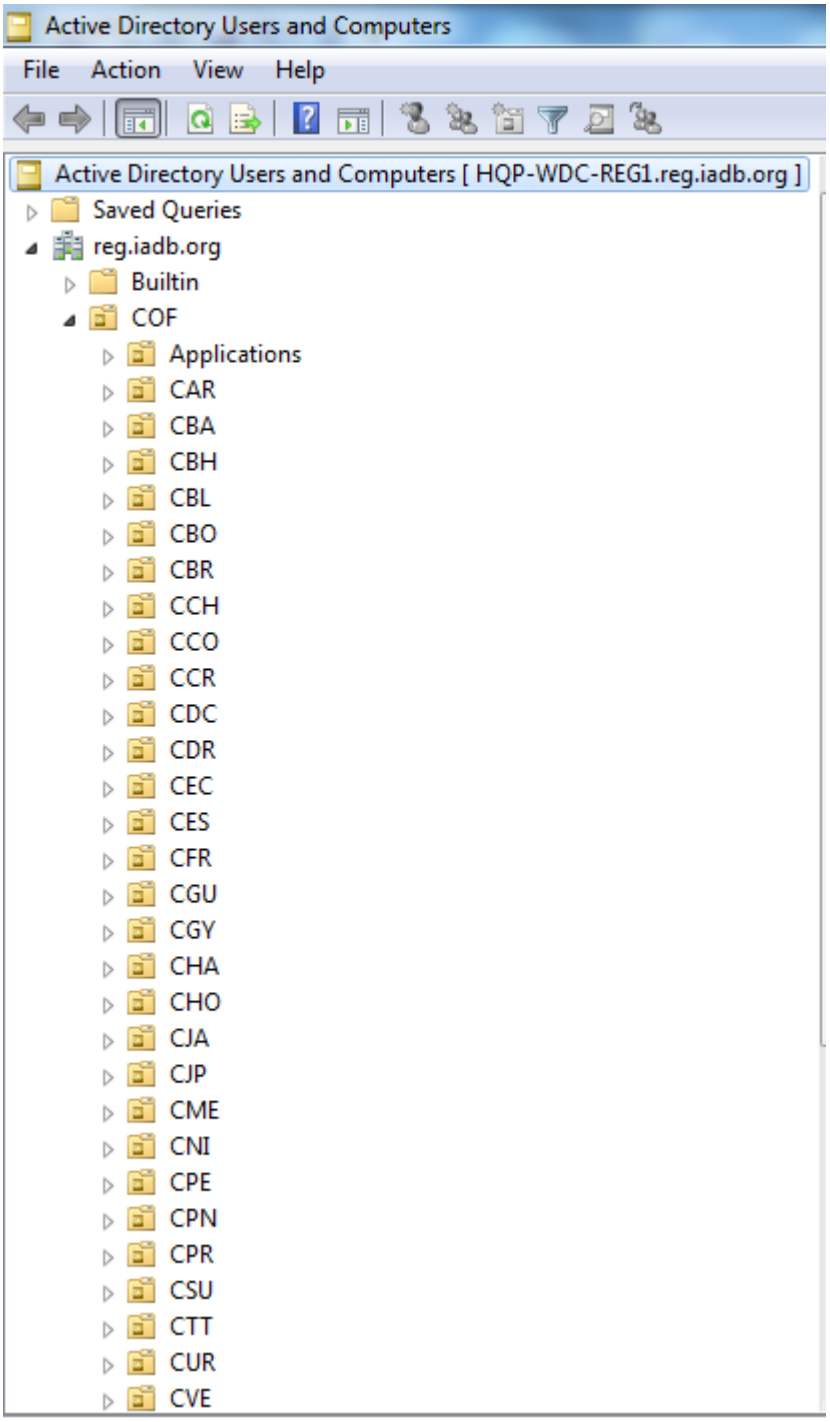


Figura 40 Mapas de AD

Politicas de Password

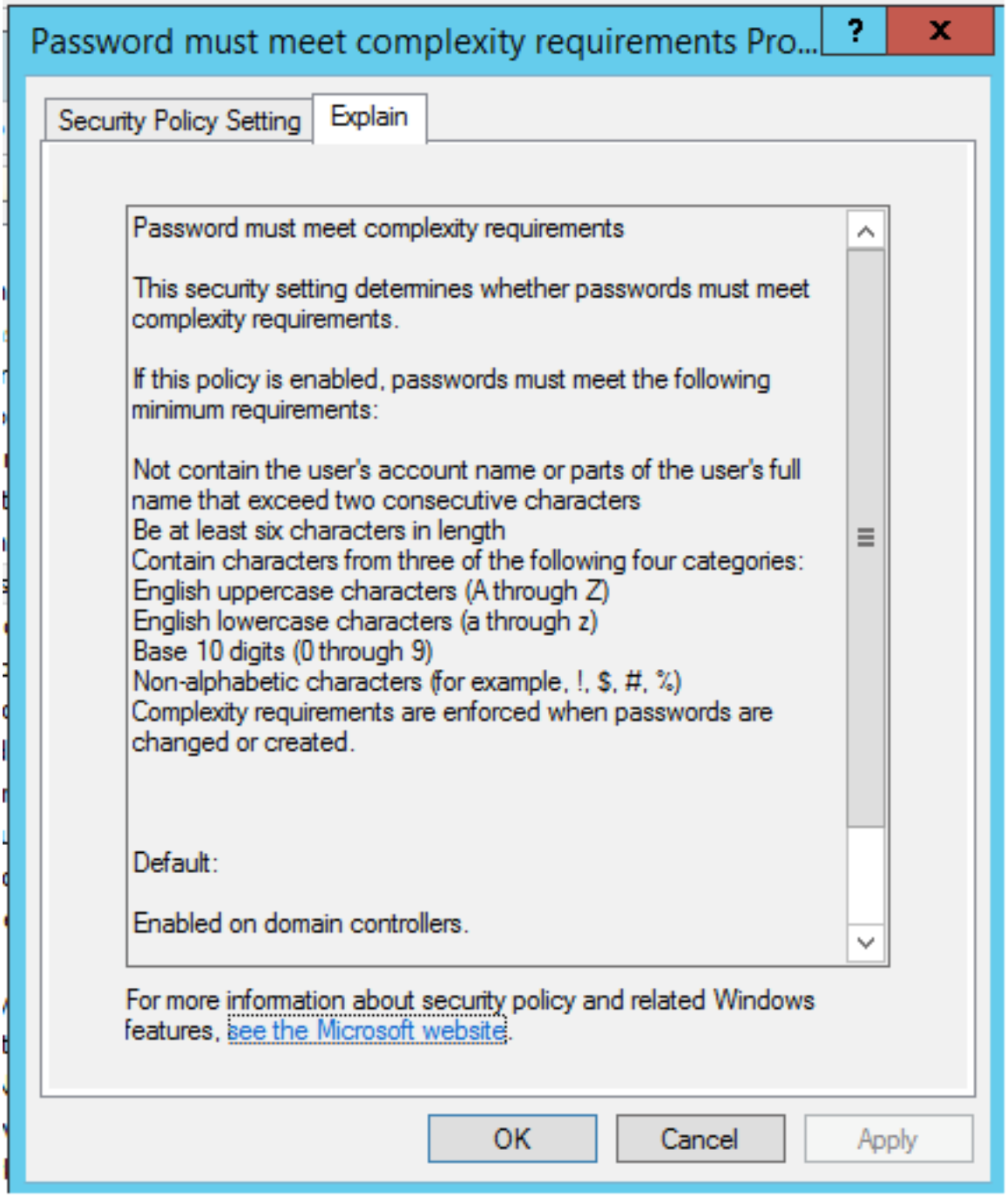


Figura 41 Politicas de Password

112

10 Plantillas de creación de roles

Los Templates se utilizan para crear la configuración que los roles de provisioning tendrán en Active directory y correo electronico. Los templates se crean en la aplicación Provisioning Manager(IDM)

Los templates se crean en Provisioning Manager

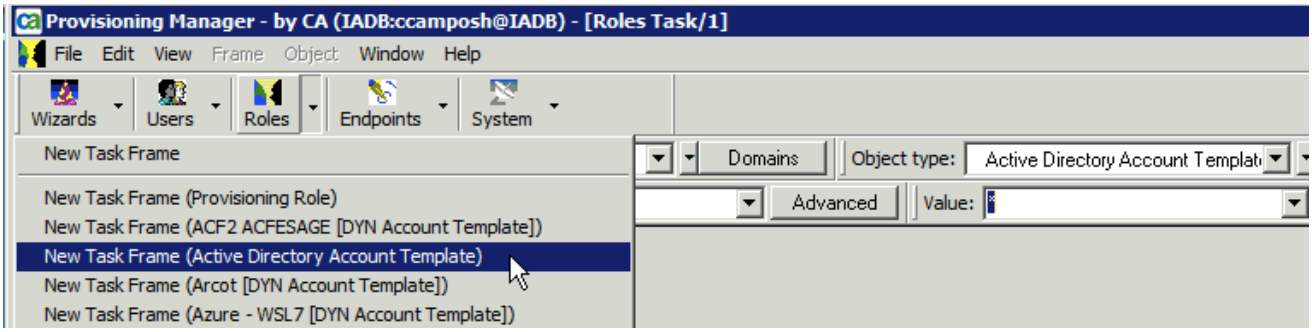


Figura 42: creación de roles

Se escoge un nombre relacionado con la unidad para la cual se utilizará el template/plantilla, en este caso la Org/Unit es ITE

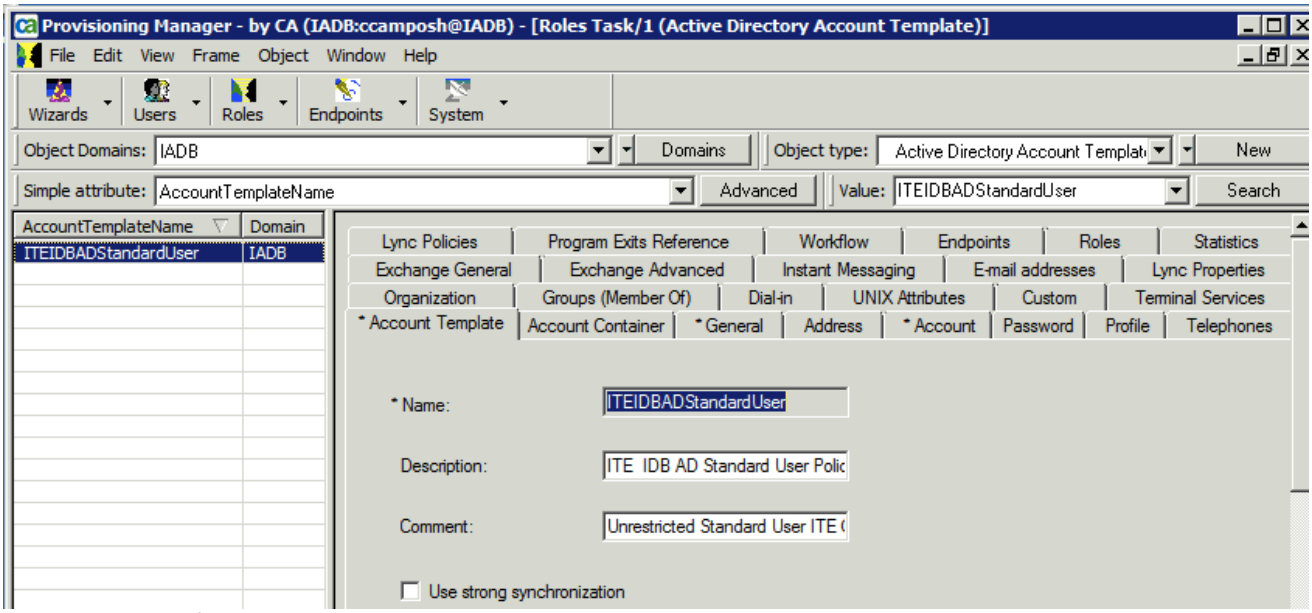


Figura 43: creación de roles

113

El template configura la conexión con el servidor y la base de datos de Exchange, para el ejemplo de esta pantalla el Mail server es: HQPAMAIL12 y la base de datos es MBX01. La aplicación Provisioning Manager se conecta con dos servidores y cuatro bases de datos de Exchange.

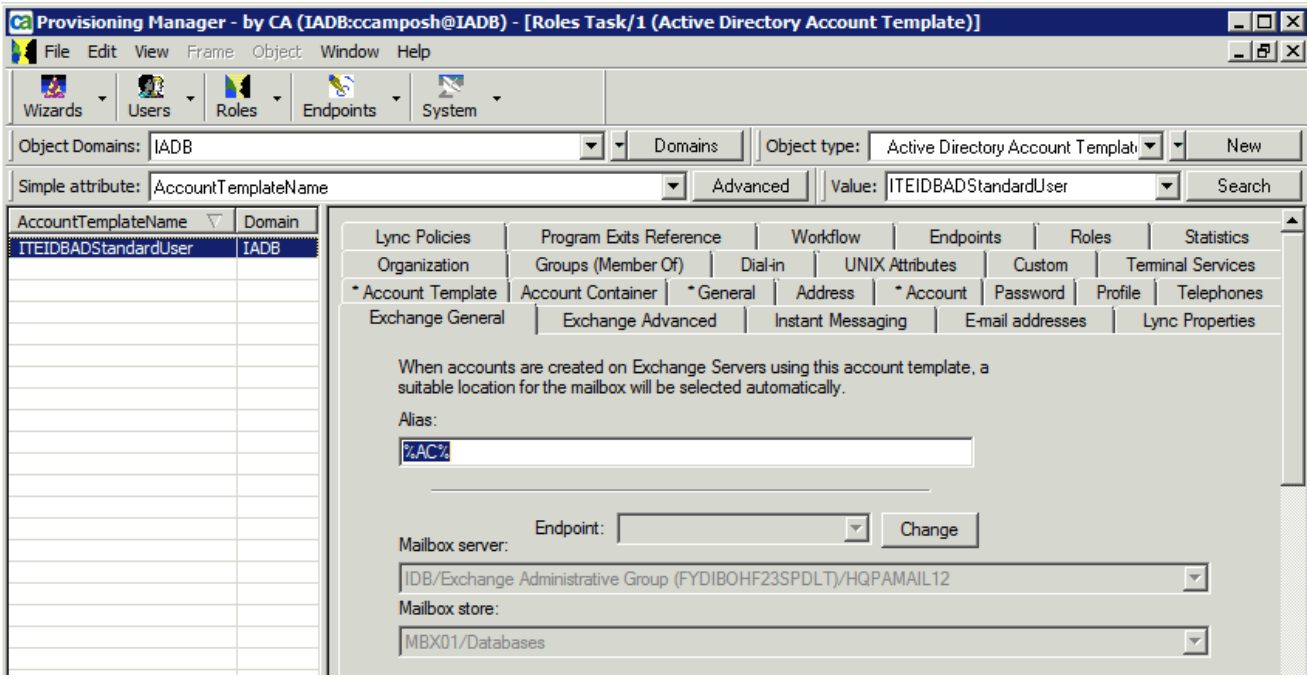


Figura 44: creación de roles

114

El template de la Org Unit ITE se conecta al endpoint IDBASH1, La unidad ITE pertenece al dominio IDB por lo que el endpoint debe ser IDBASH1.

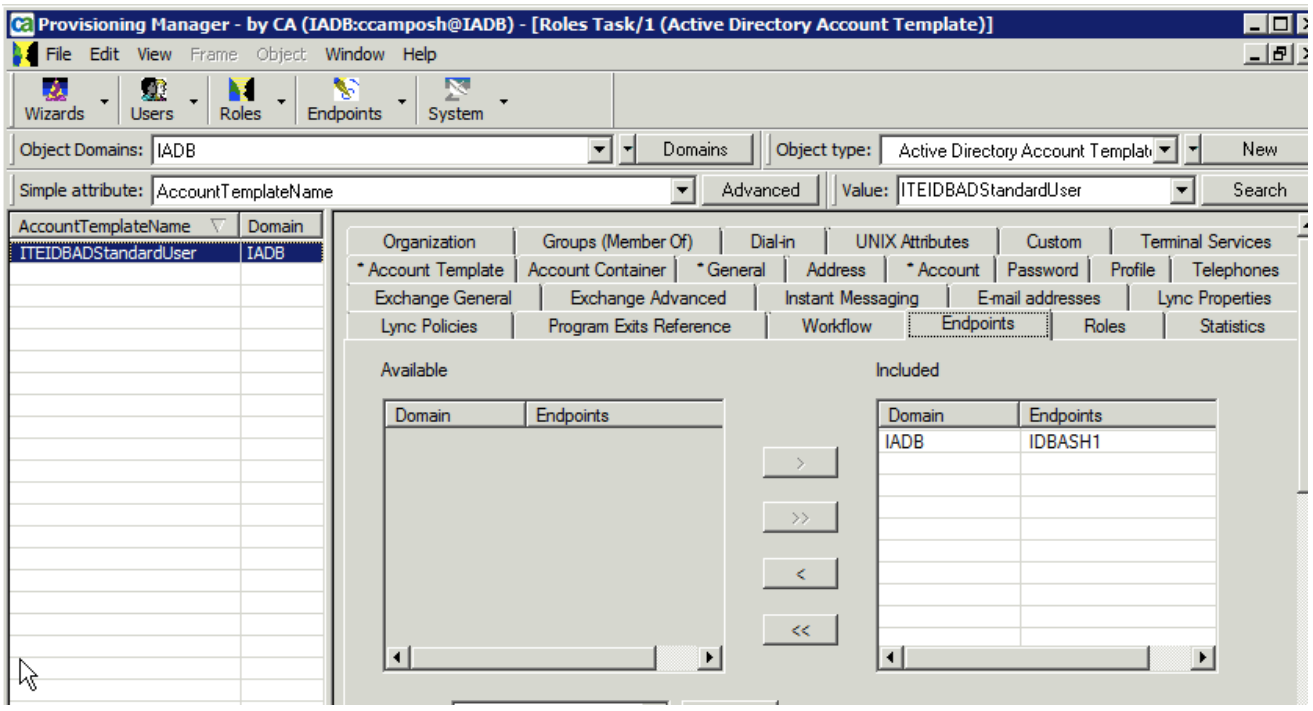


Figura 45: creación de roles

115

El role que se asigna al template de ITE es el role relacionado con la unidad ITE, el role se llama IDBStdUserADMail_ITE. Las cuentas de AD y de correo se crean mediante roles. Los roles se utilizan en el provisioning process.

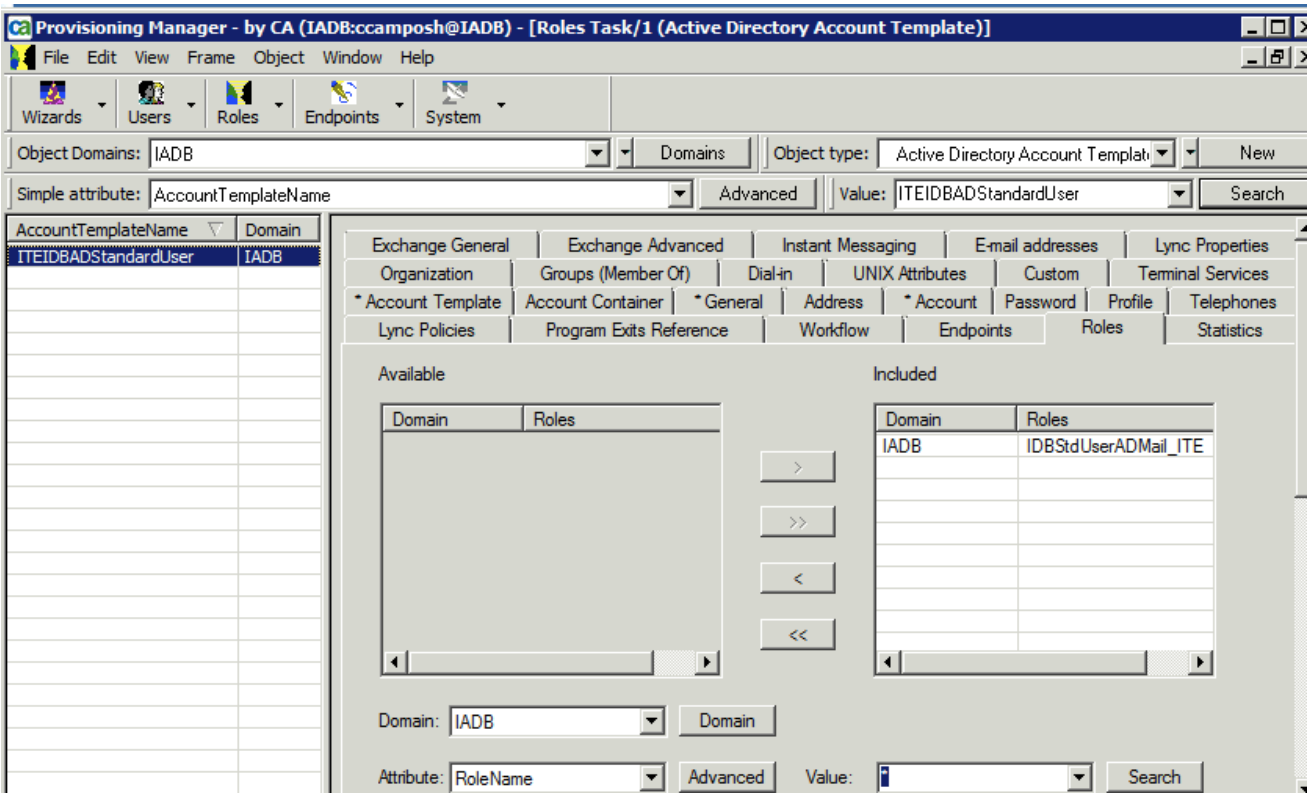


Figura 46: creación de roles

116

Tambien el Template asigna grupos de Active Directory de acuerdo a la unidad organizacional, en este caso el template de la unidad ITE se le asigna el grupo llamado ITE, el folder de ITE en active directory se llama HQ/ITE/Groups

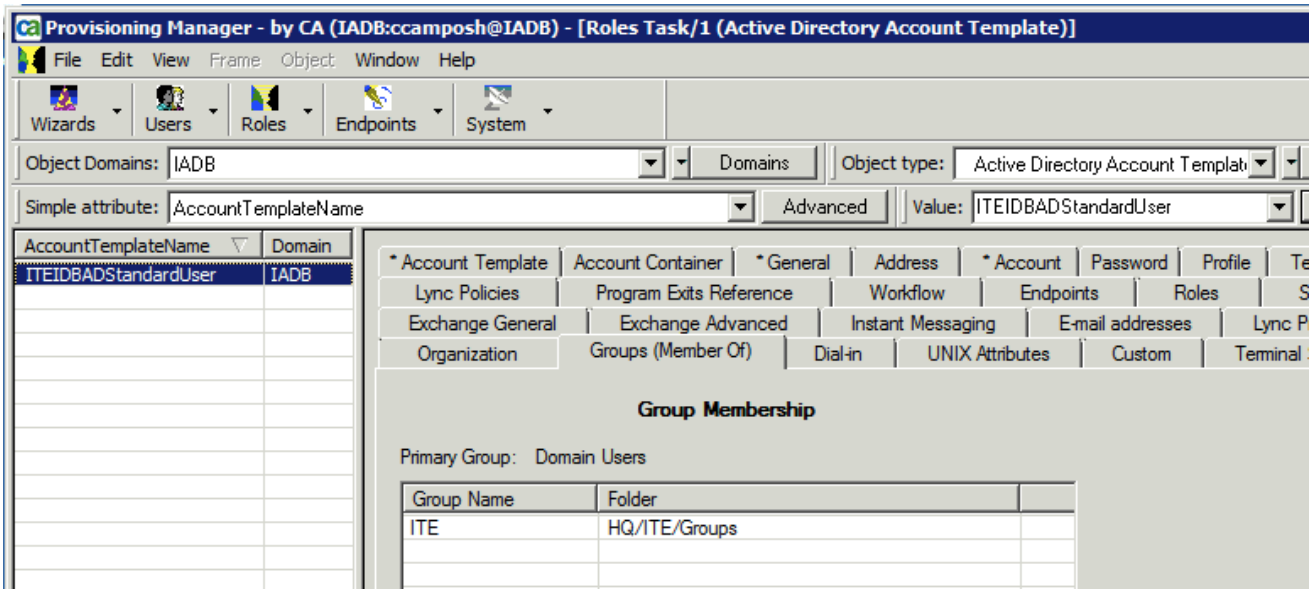


Figura 47: creación de roles

117

El template también asigna atributos en Active Directory, en esta pantalla el template asigna el atributo de employeeID(número de empleado) y asigna el atributo número 1 que significa el tipo de empleado, puede ser Staff, Contractor or Contractual.

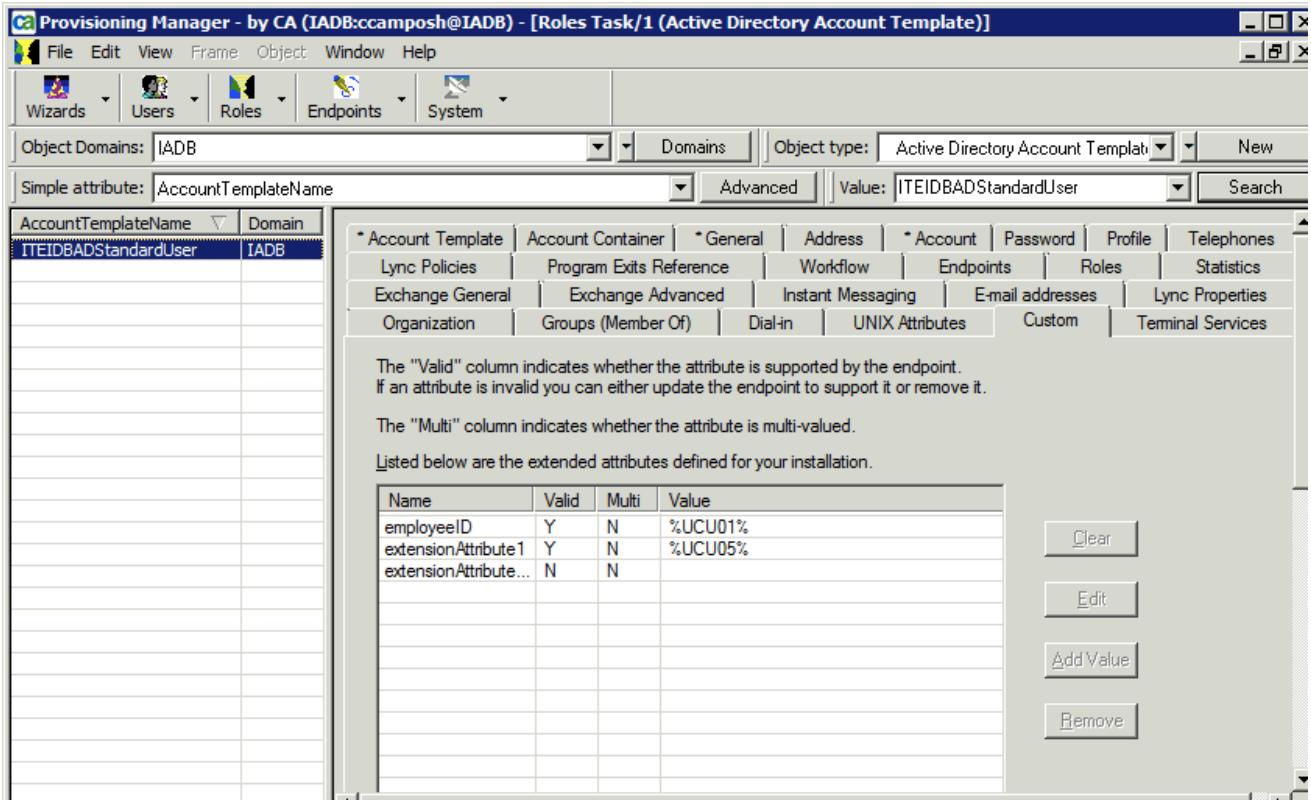


Figura 48: creación de roles

118

El sistema de provisioning crea las cuentas de Active Directory por medio de roles y templates y las asigna en los folders de Active directory de acuerdo a las Unidad Organizacional, las cuentas se colocan en Users dentro de los folders.

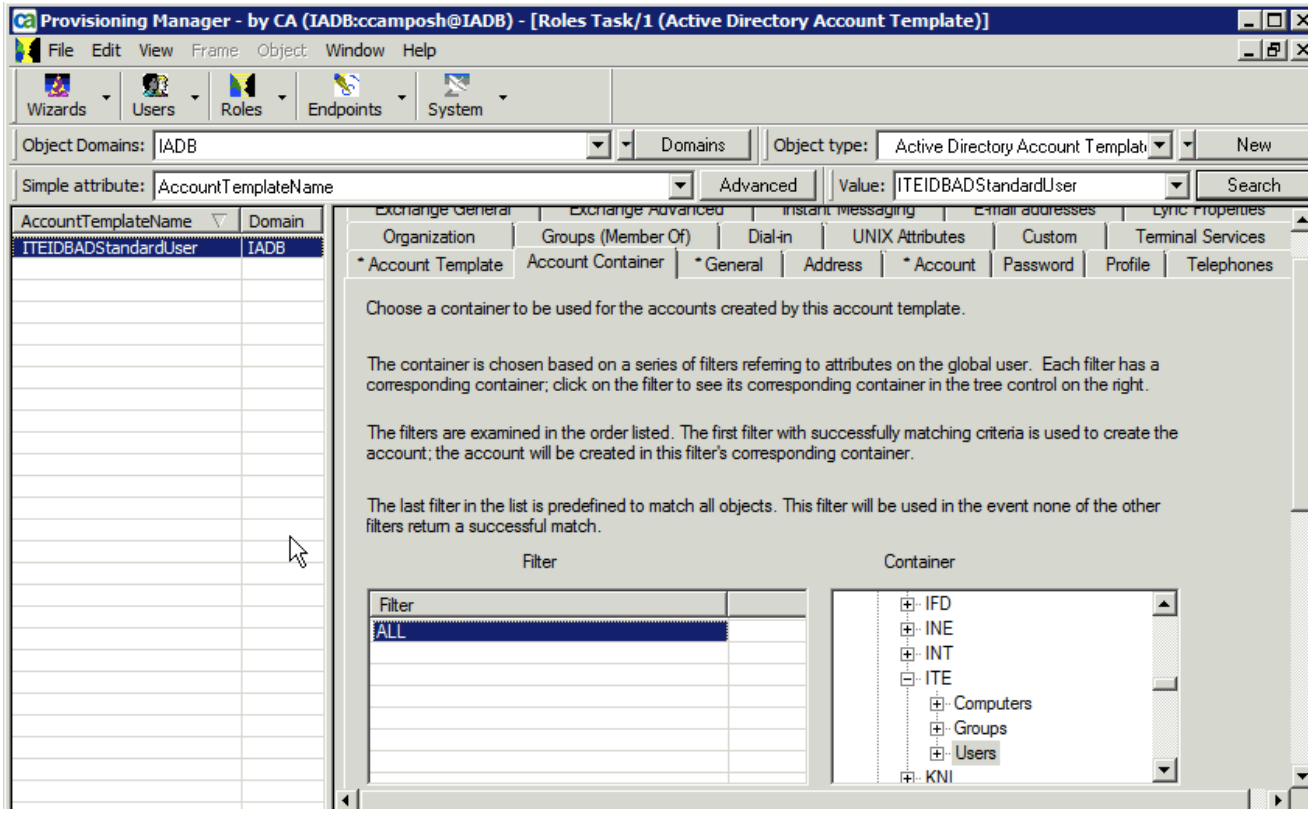


Figura 49: creación de roles

119

Las cuentas de Active Directory se crean activas

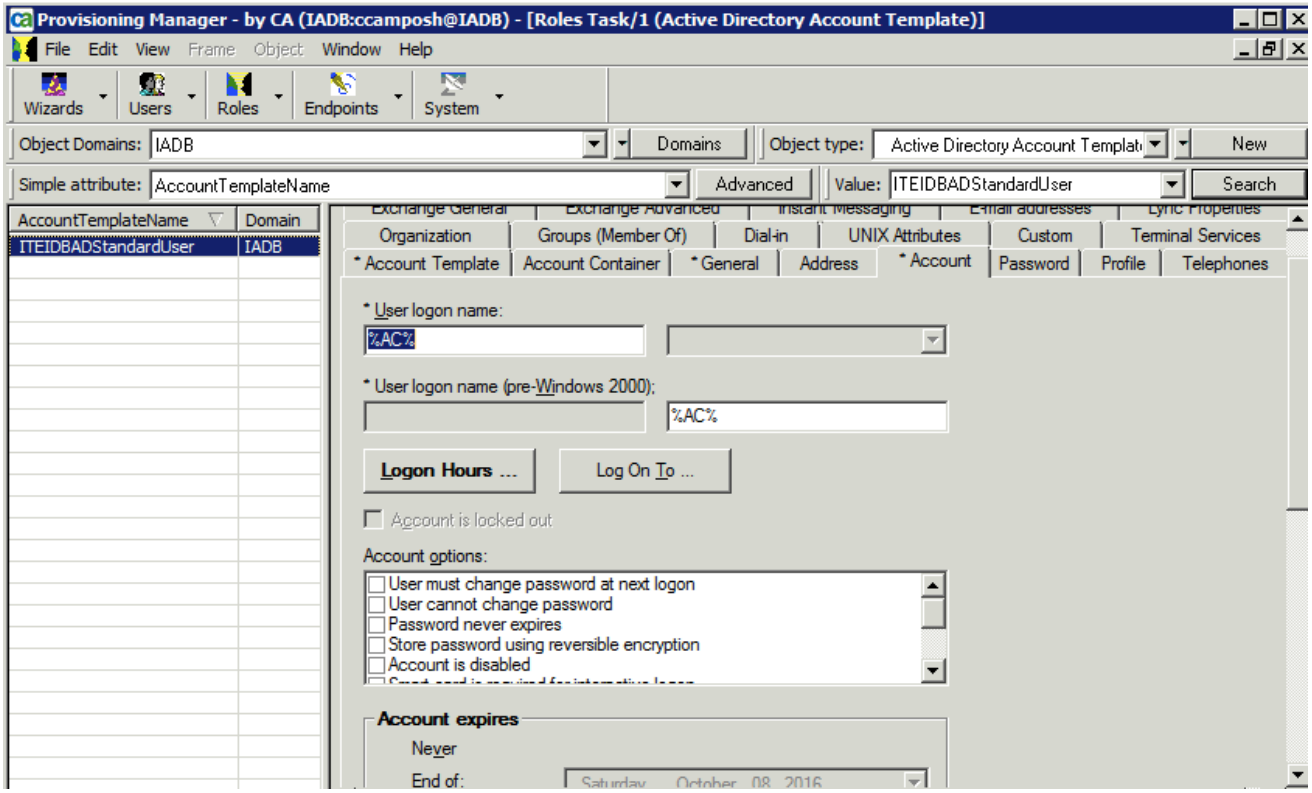


Figura 50: creación de roles

11 Creación de roles

Los roles son los que ejecutan los eventos de Provisioning(Nuevo Usuario, Terminación, recontratación y transfer) y los roles contienen pantillas, las plantillas son las que vimos en el segmento anterior.

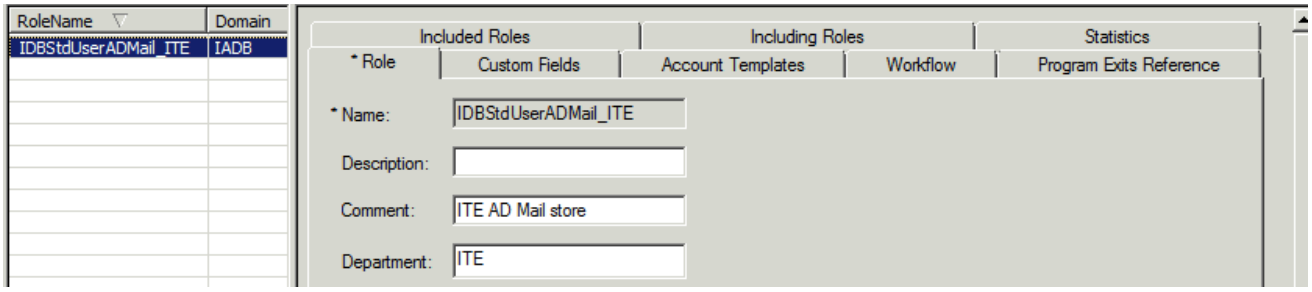


Figura 51: creación de roles

En la pantalla de abajo se muestra como se asigna una plantilla a un role

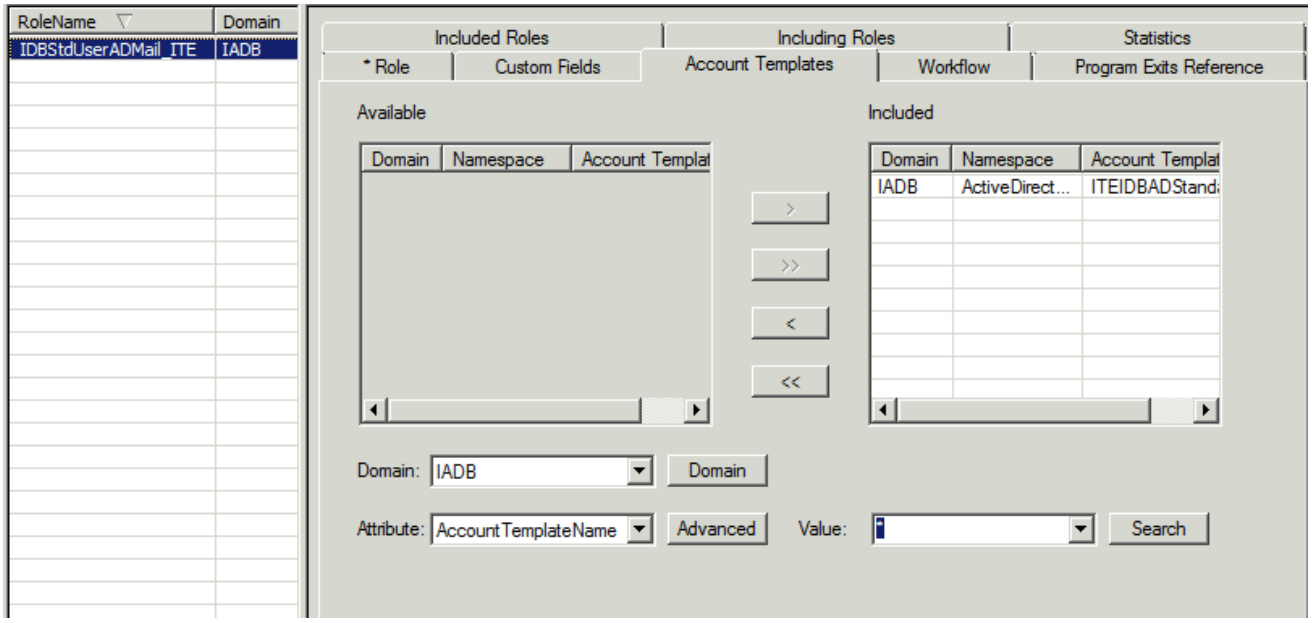


Figura 52: creación de roles

12 Guia de Operación de Identity Minder

Arquitectura de Identity Minder

El proyecto de aprovisionamiento de CA Identity Minder en el IADB involucre varios de los componentes siguientes:

- Servidores – CA Identidad Minder, CA Provisioning Manager, CA Siteminder, IAM Servidor de reportes, IIS Web Servicio.
- Almacenamiento de usuarios – Directorio de Provisioning, Directorio corporativo
- Base de datos – MS SQL Server 2008 cluster, usado por Identity Minder/Siteminder/Report Server
- Endpoints – Active Directory, CA Access Control, Servidor de Oracle, MS Exchange Server 2010(con agente remoto CA)

La ilustración mostrada a continuación cuenta con todos los componentes trabajando juntos para entregar una solucion completa de IDM(Identity Minder)

122

Ambiente de producción

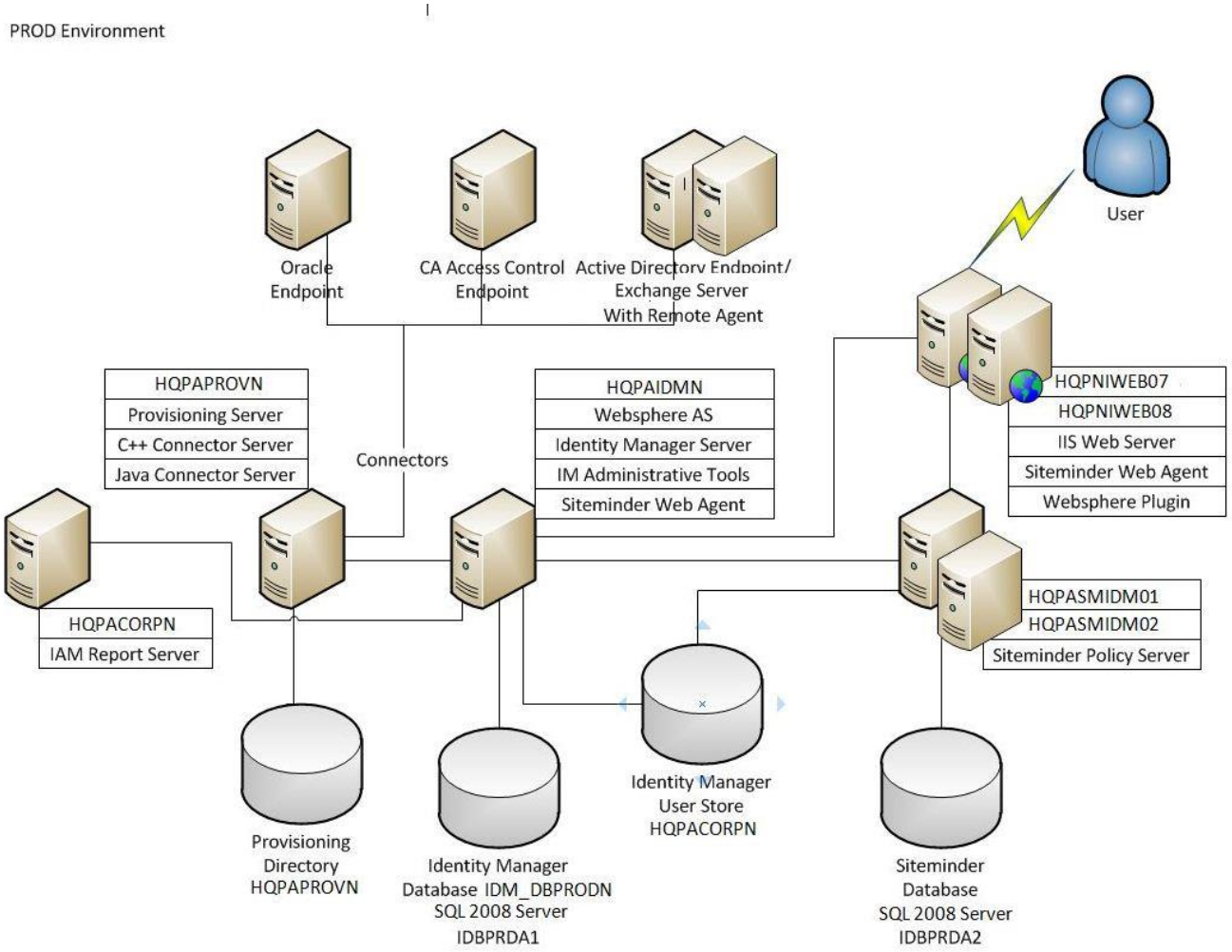


Figura 53: Ambiente de producción del proceso de provisioning

Ambiente de Pruebas

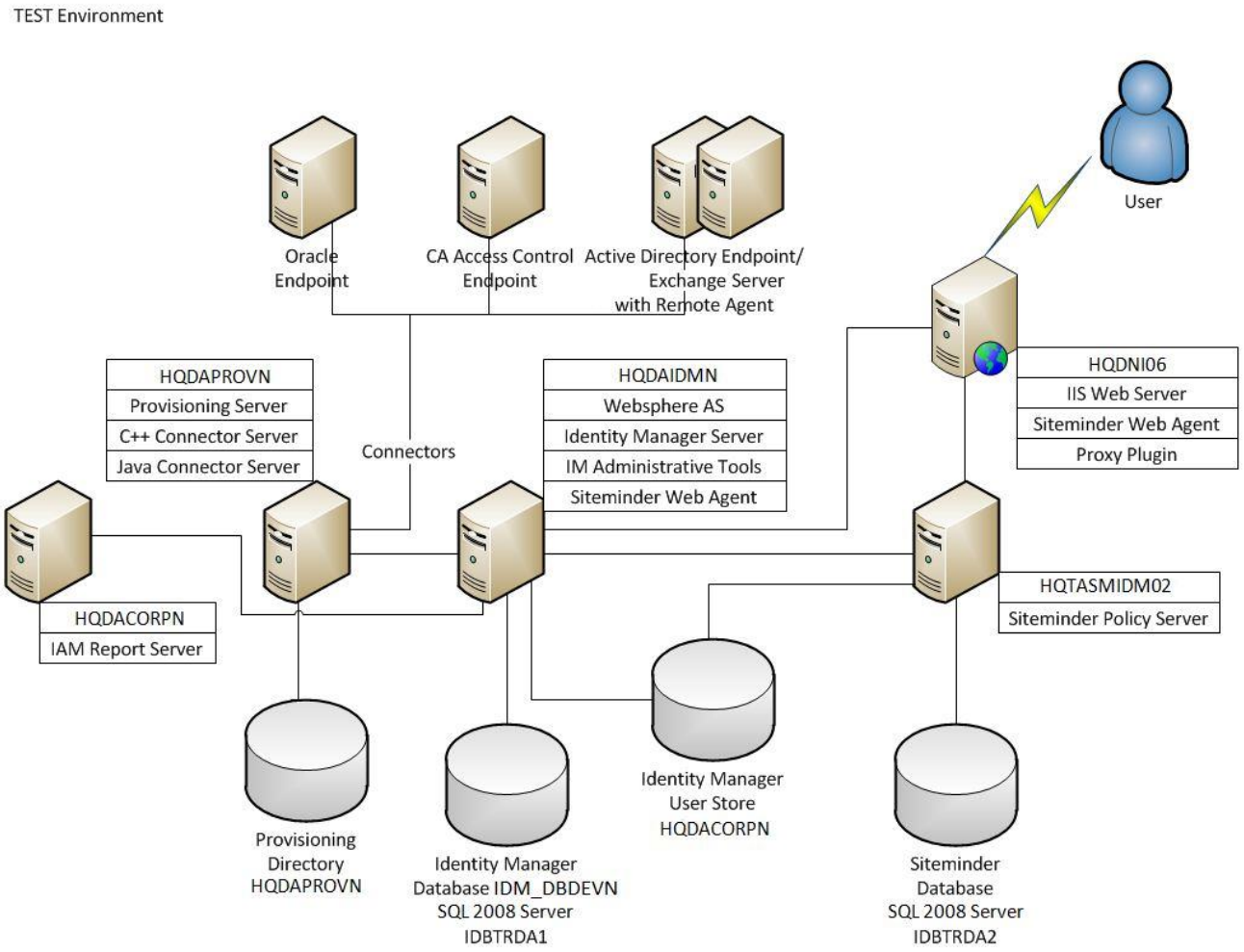


Figura 54: Ambiente de pruebas del proceso de provisioning

124

13 Servicios Criticos (ver tabla 32)

Tabla 32 – Servicios Criticos

Nombre del servidor	Nombre servicio de pantalla	Nombre del servicio	Descripcioón del servicio
HQPNIWEB07/08 (Producción) HQDNI06 (Prueba)	IIS 7.0 Servicio	Información de servicio de internet	Arranque Automatico Reiniciar IIS también reinicializa agente web SM
HQPAIDMN (producción) HQDAIDMN (prueba)	IBM Websphere Servidor de aplicaciones V7.0 - HQPAIDMNNode01	IBMWAS70Servicio-HQPAIDMNNode01	Ejecuta aplicaciones Websphere Servidor Tipo arranque: automático
HQPAPROVN (producción) HQDAPROVN (prueba)	CA Identity Minder-servidor de aprovisionamiento Abreviación:	IM_PS	Servidor de arranque Controlador de abastecimiento Tipo de Arranque: Automático
HQPAPROVN (producción) HQDAPROVN (prueba)	CA Identity Minder-Conector de Servidor (C++)	IM_CCS IM_JCS	Ejecuta servidores de mensajeria instantanea IM servidores de conector y directorios de aprovisionamiento.

125

	CA Identity Minder-Java Conector de Servidor (JCS) Servicios de directorio de aprovisionamiento	HQDAPROVN-impd-co HQDAPROVN-impd-inc HQDAPROVN-impd-main HQDAPROVN-impd-notify HQDAPROVN-router	Tipo de arranque: Automatico
HQPACORPN (producción) HQDACORPN (prueba) Report Server Tomcat Apache Servidor Business Objects Server Intelligence Agent	IADBCorp usuario de arranque, servicio DSA Apache Tomcat (en panel de servicios) En Business Central Controlador de configuración	IADBCorp Apache Tomcat	Tipo de arranque: Automatico

Bases de datos y Endpoints (ver tabla 33)

Tabla 33 – Bases de datos y Endpoints(Pruebas)

Base de datos de hospedaje	Instancia de base de datos	Nombre de base de datos	puerto

126

idbtrda1 (IDM Almacen de objetos, Tarea persistente, Auditoría DB, Flujo de trabajo, Archivo db)	idbtrda1inst1	idm_dbdevn	2974
idbtrda1 (Reportes DB, Capturas instantaneas DB)	idbtrda1inst1	IDM_REPDEVN	2974
IDBTRDA2 (Siteminder Politica de almacen DB)	IDBTRDA2INST2	SMIDMDBTST	3188

127

Bases de datos y Endpoints (ver tabla 34)

Tabla 34 – Bases de datos y Endpoints(Producción)

Base de datos de hospedaje	Instancia de base de datos	Nombre de base de datos	puerto
idbprda1 (IDM Almacen de objetos, Tarea persistente, Auditoría DB, Flujo de trabajo, Archivo db)	idbprda1inst1	IDM_DBPRODN	1518
idbprda1 (Reportes DB, Capturas instantaneas DB)	idbprda1inst1	IDM_REPPRODN	1518
IDBPRDA2 (Siteminder Politica de almacen DB)	IDBPRDA2INST2	SMIDMDBPRD	1757

Endpoints Información (Ver tabla 35)

Tabla 35 – Endpoints Información (Prueba)

Namespace	Endpoints
Directorio Activo	TESTIDB
CA Controles de acceso	VDEVAPPS1 VDEVDBMS1 VDEVWEB1
Oracle Endpoint	BEATST FIETEST FINTST LAWSTAGE LMSTST PSTEST TMSTSTS

Endpoints Innformación (ver tabla 36)

Tabla 36 - Endpoints Innformación (Producción)

Namespace	Endpoints
Directorio Activo	IDBASH1 IIC REGASH
CA Controles de Acceso	PMDB_PRDAPPS PMDB_PRDDBMS PMDB_PRDWEB TSTAPPS1 TSTDBMS1 TSTWEB1
Oracle Endpoint	BEAPRDB BEATST BIDPRD BIDTST BMSPROD BMSTEST CMSPRD CMSTST EDWPRD EDWTST FIEPROD FIETEST FINPRD FINTST IMSPRDS IMSTSTS LAWPROD LAWSTAGE LMSPRD LMSTST PSPROD PSTEST

129

14 Componentes de Identity Minder

14.1 Servidor de Identity Minder

La aplicación J2EE Identity Minder incluye la consola de manejo y la consola de usuario

La Identity Minder consola de manejo es una web es una herramienta basada en Web para la creación de un directorio de Identity Minder , la configuración de un entorno de Identity Minder , la asignación de un administrador del sistema , y la habilitación de funciones personalizadas.

URL de Producción:

http://newidm.iadb.org/iam/immanage

URL de pueba:

http://idmt.iadb.org/iam/immanage

14.1.1 Entornos Identity Minder

Inicia sesión en la consola de administración de mensajería instantánea para crear los directorios y los IME para el sistema.

Prod IME : IADBProv

IME prueba: aprovisionamiento de desarrollo

14.1.1.1 Crear directorios

Para la creación de directororios se siguen los pasos descritos en las figuras 22 a la 28.

130

Captura de pantalla para creación de directorios, paso 1.

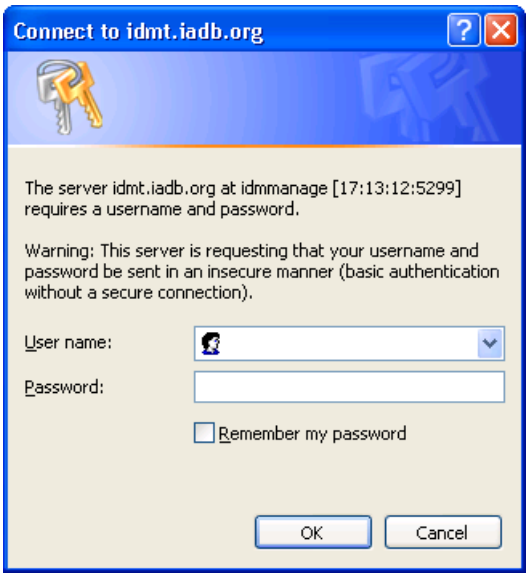


Figura 55: creación de directorios

Pulsa en Directorios, paso 2.

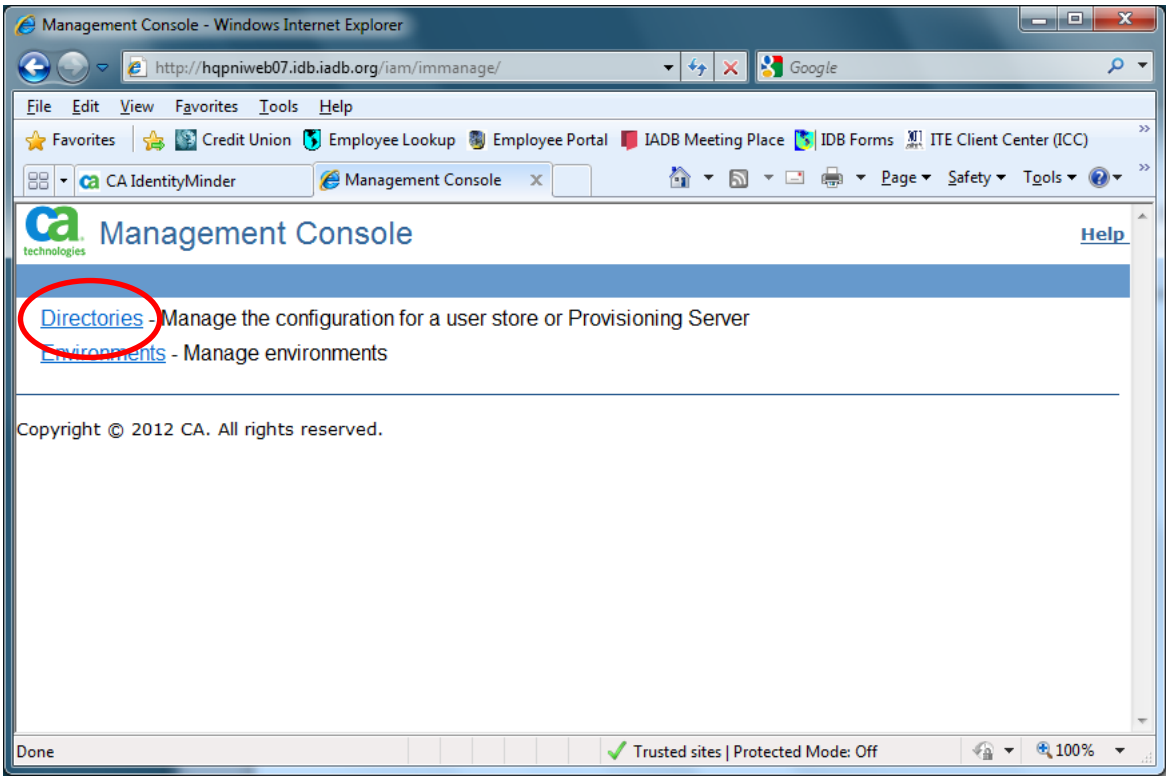


Figura 56: creación de directorios

131

Pulsa en Nuevo, selecciona tu archivo directorio.xml, Paso 3

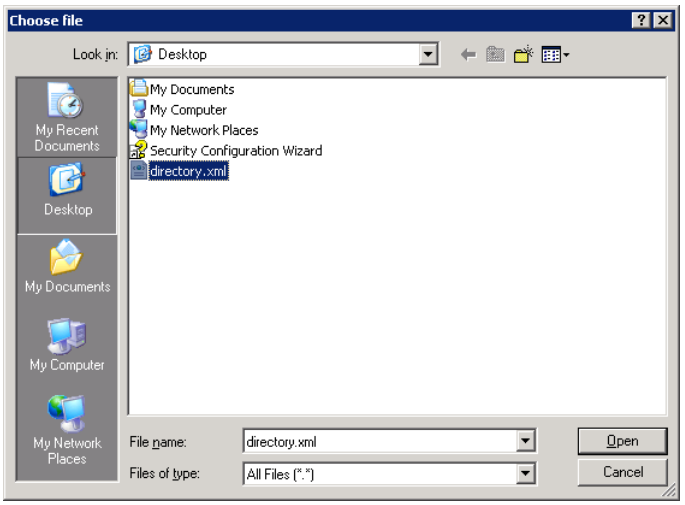


Figura 57: creación de directorios

Click en Siguiente

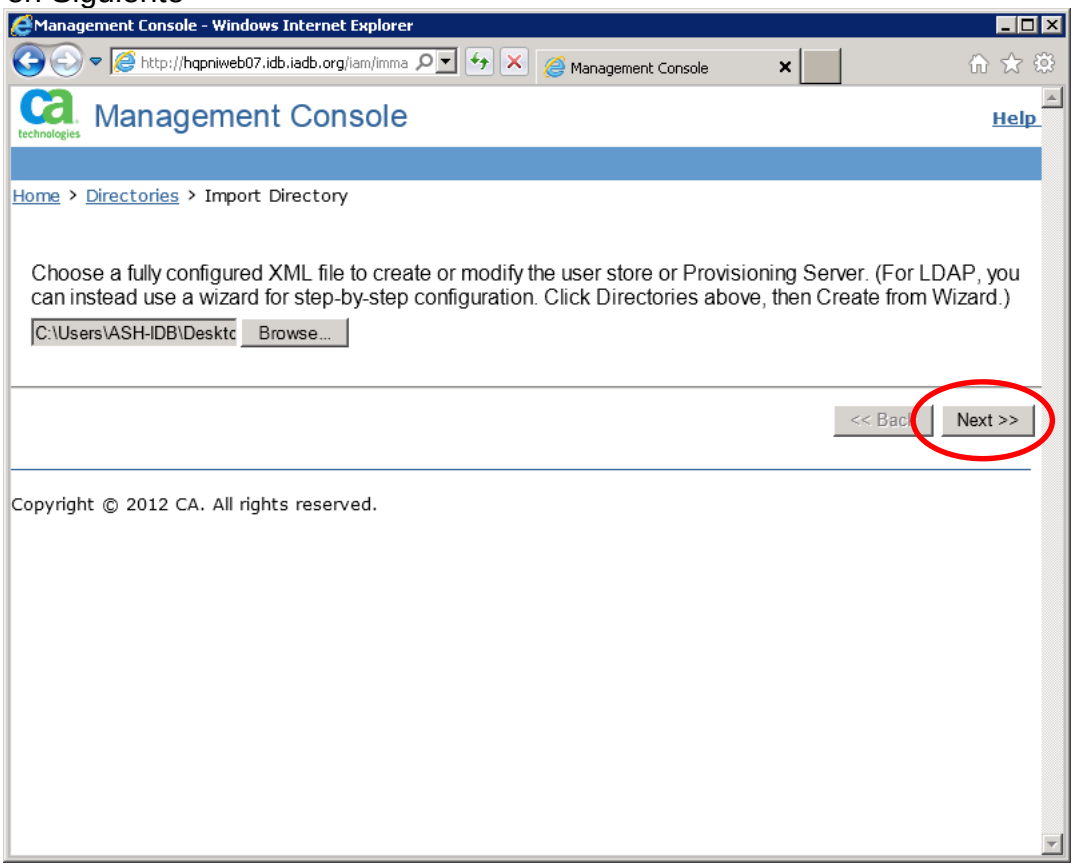


Figura 58: creación de directorios

132

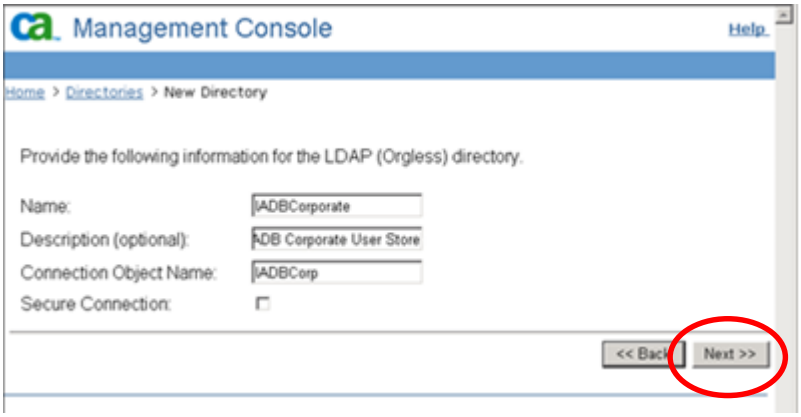


Figura 59: creación de directorios

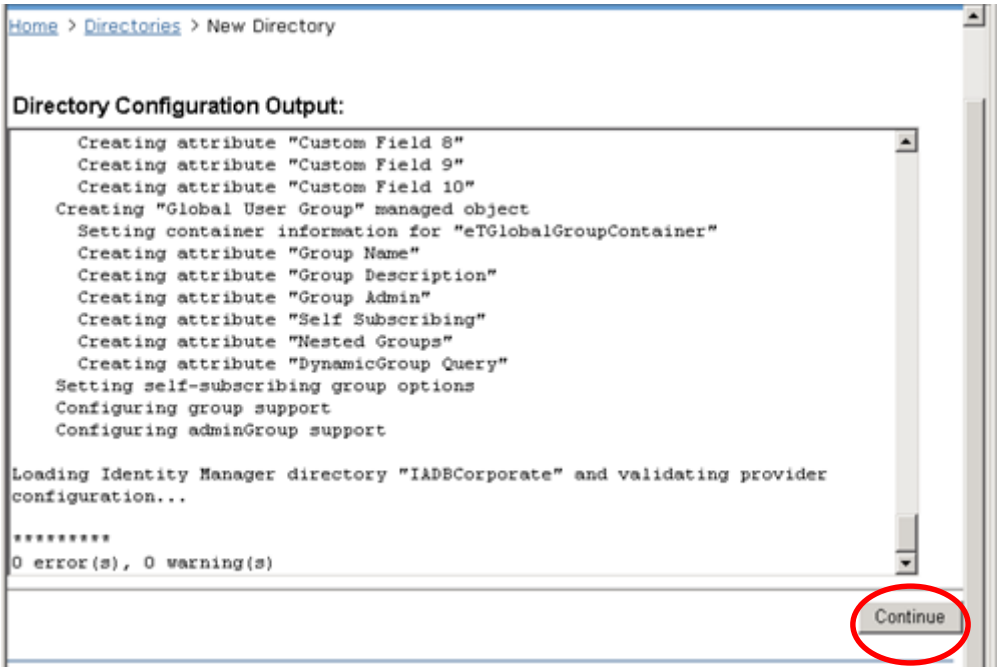


Figura 60: creación de directorios

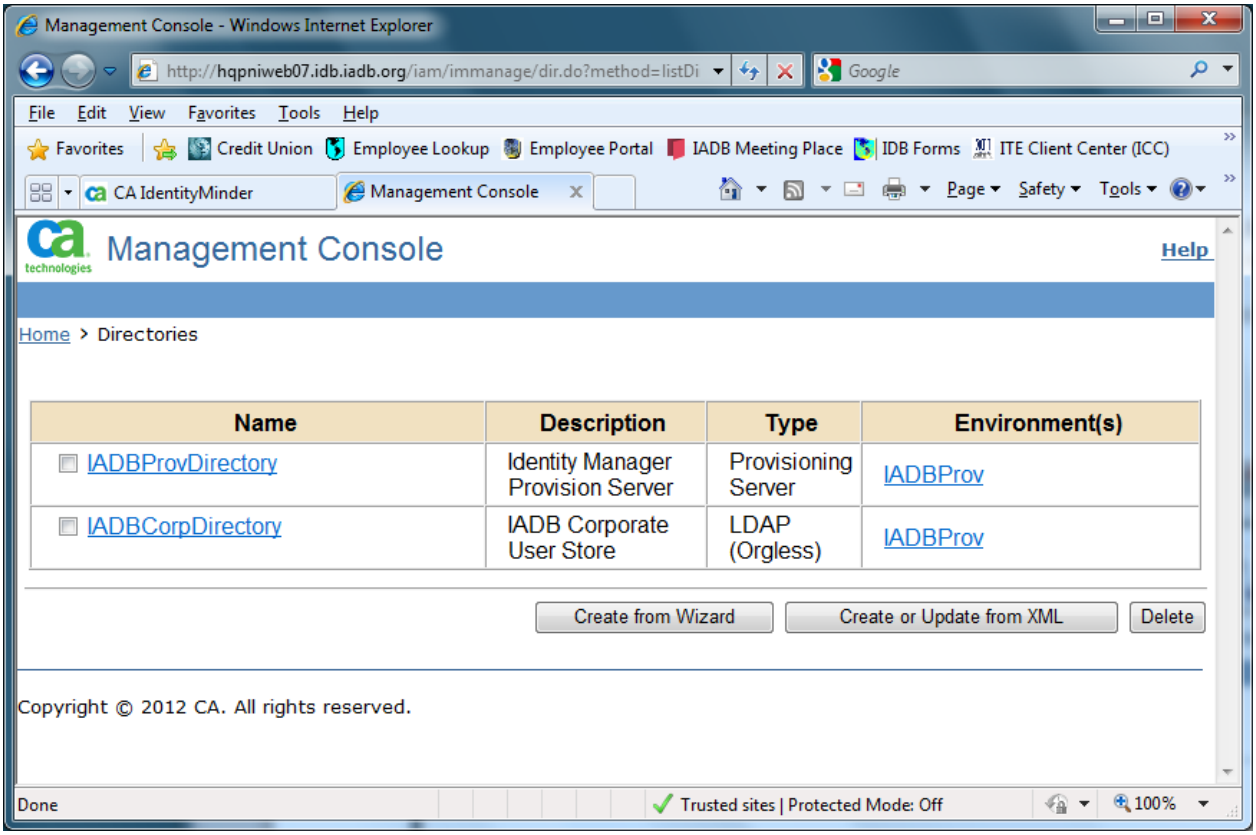


Figura 61: creación de directorios

Siga los pasos anteriores para crear todos los directorios necesarios

Directorios de producción:

IADBCorporate

Server: HQPACORPN

Port: 2389

Abastecimiento IADB

Servidor: HQPAPROVN

Puerto: 20389

Directorio de pruebas:

Directorio de prueba corp

Servidor: HQDACORPN

Puerto: 2389

Directorio de prueba prov

Servidor: HQDAPROVN

Puerto: 20389

14.1.1.2 Crear entornos de Identity Minder

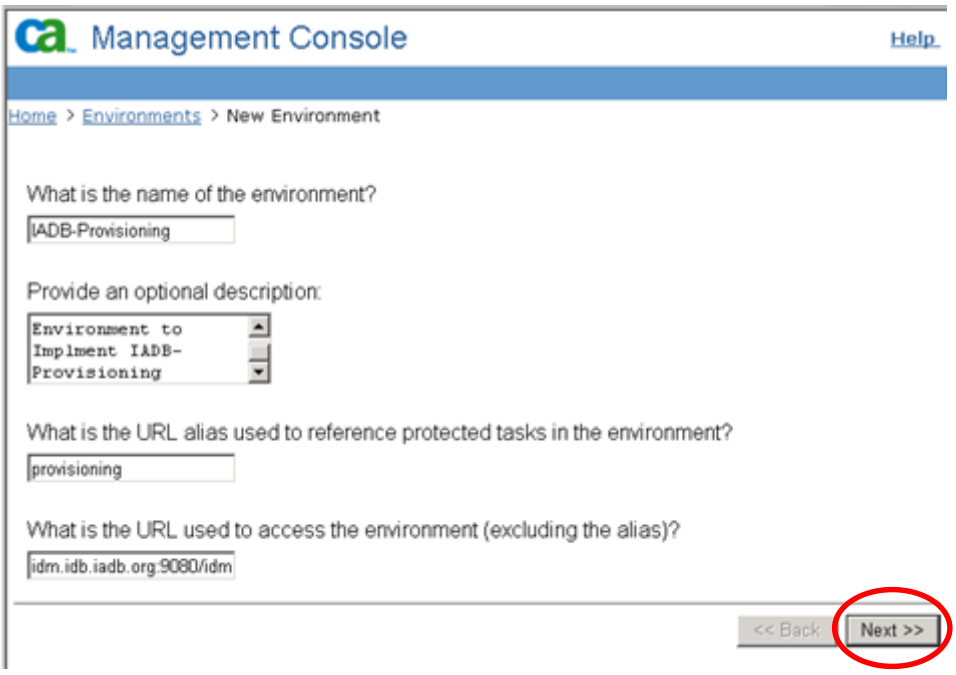


Figura 62: creación de entornos

135

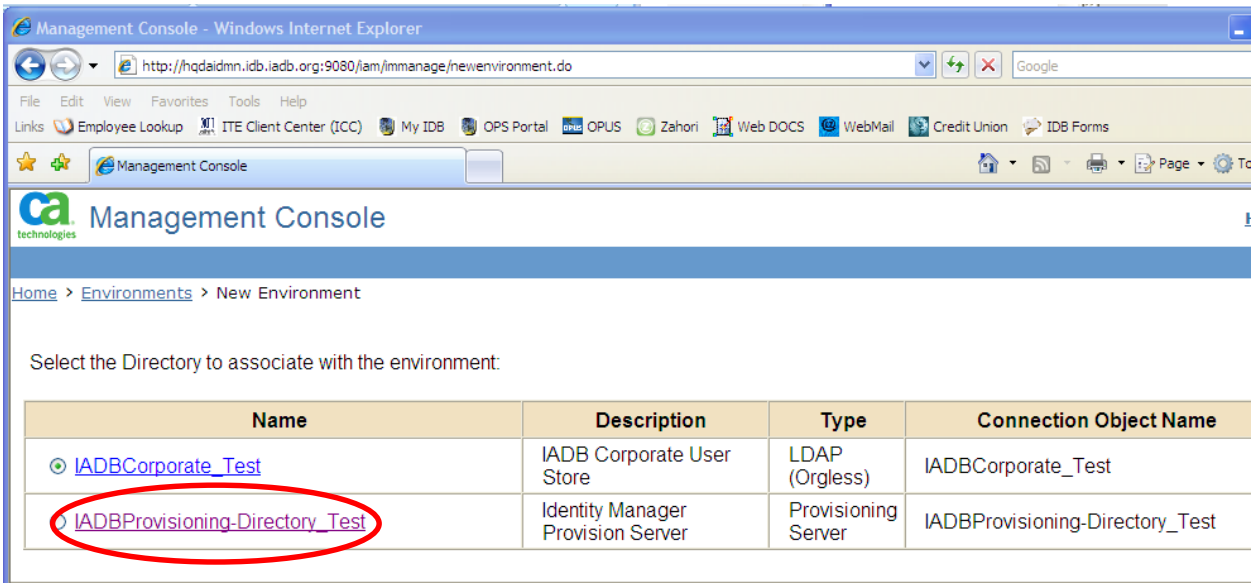


Figura 63: creación de entornos

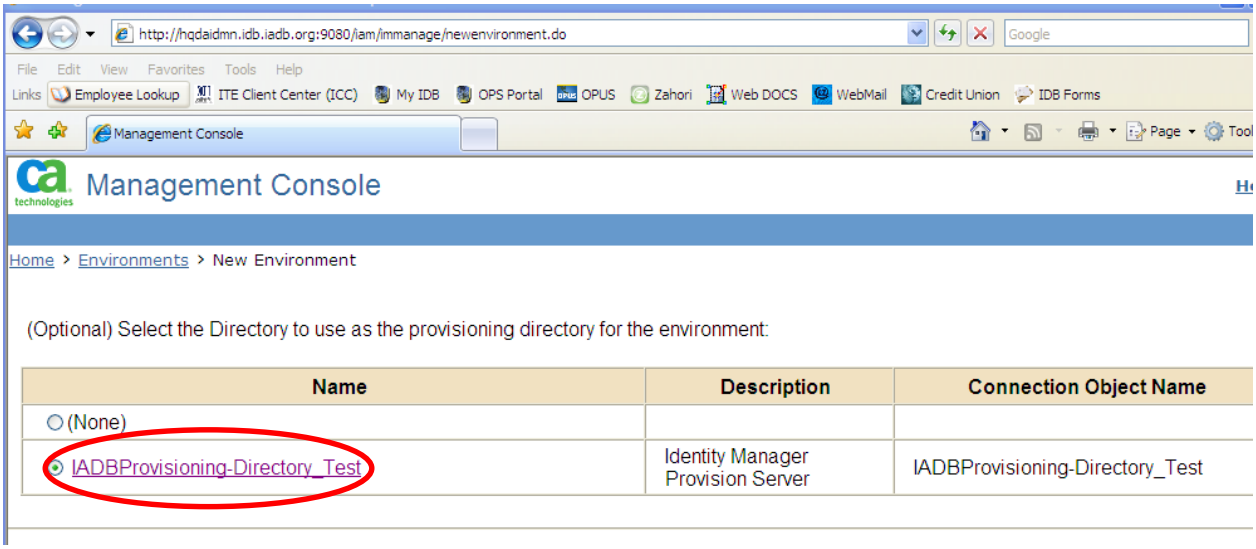


Figura 64: creación de entornos

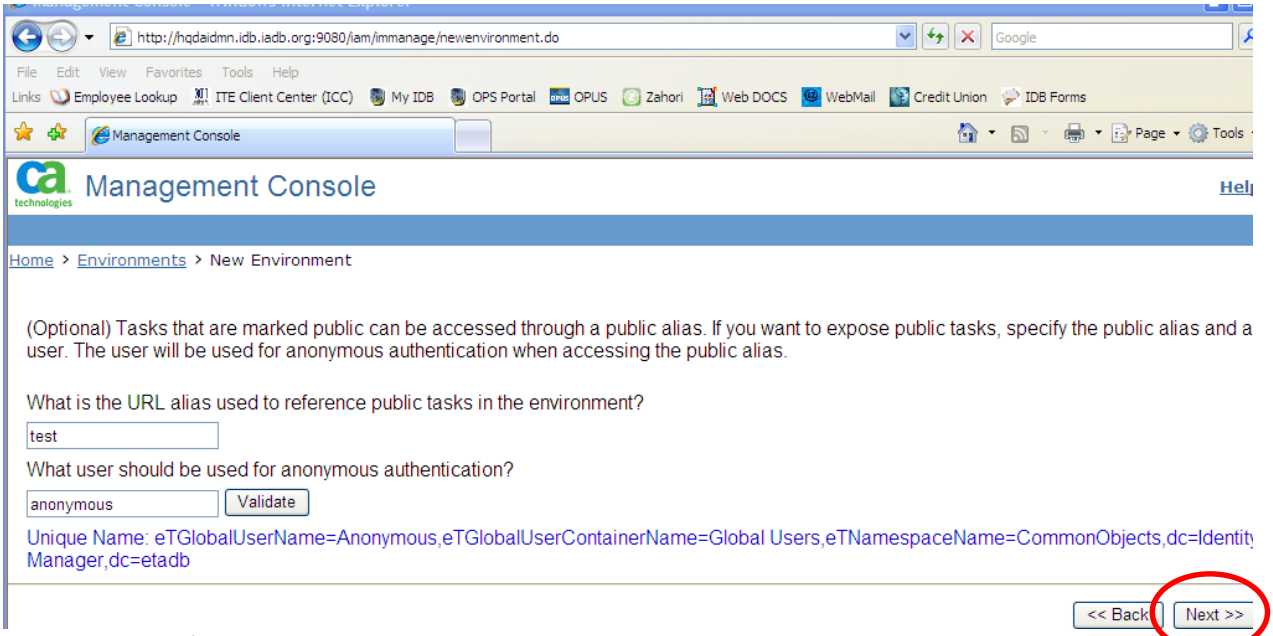


Figura 65: creación de entornos

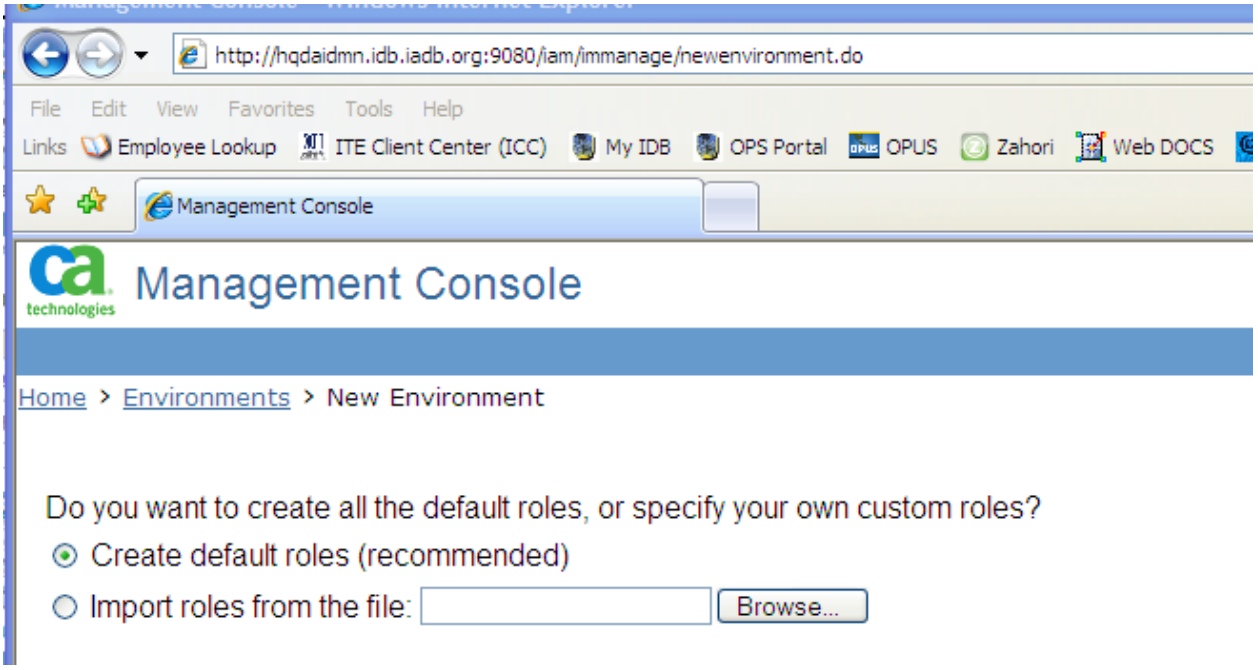


Figura 66: creación de entornos

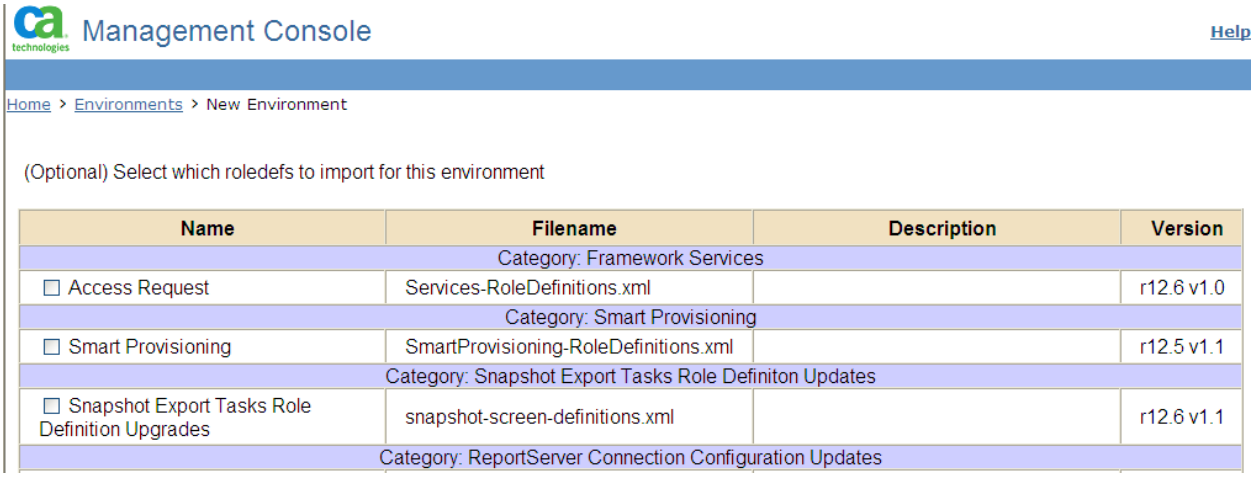


Figura 67: creación de entornos

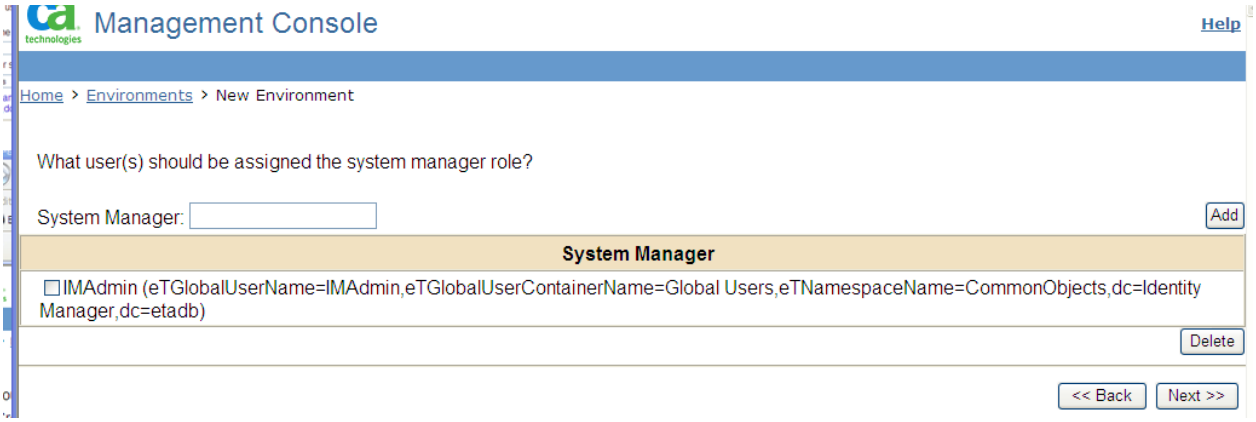


Figura 68: creación de entornos

User name – IMAdmin (for test environment)

User name – IMAdminP (for production environment)

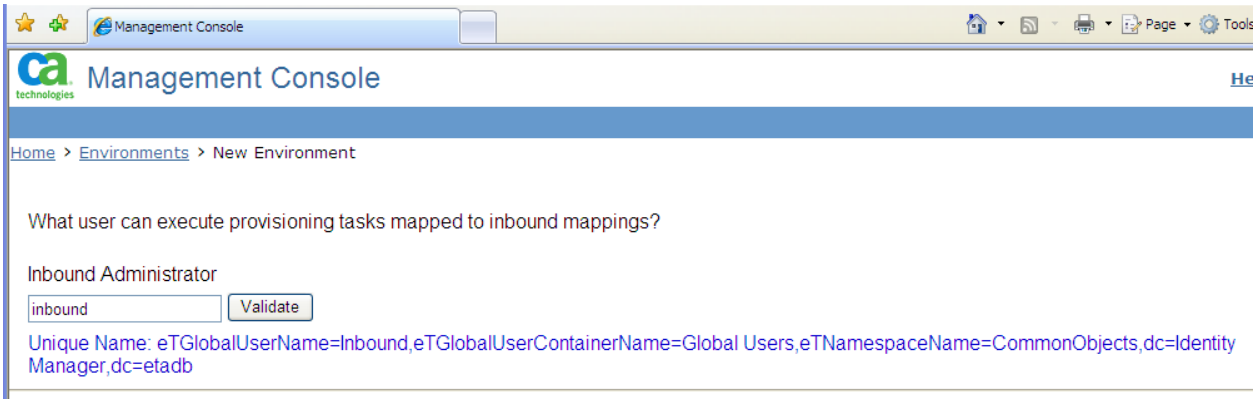
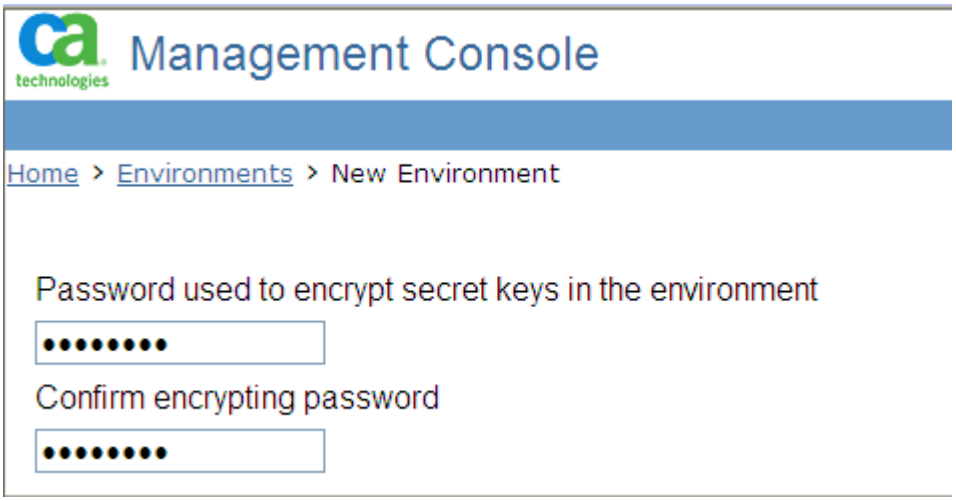


Figura 69: creación de entornos



Home > Environments > New Environment

After configuring an environment, configure the logout URI in the agent to ensure proper functionality. See the documentation for instructions.

Select the agent that will protect the installation for this environment:

Name	Agent Type	Description
BackChannelAgentGroup	AffiliateMinder (Agent Group)	AgentGroup for BackChannel communications
FederationWebServicesAgentGroup	Web Agent (Agent Group)	agent group to secure the federation webservices component.
fss ui agent	Web Agent	For Legacy/Fed
hqdni06wa	Web Agent	

A new environment will be created with the following settings:

Property	Value
Name	TeeTest
Description	
Protected Alias	testing
Base URL	http://hqdaidmn.idb.iadb.org:9080/iam/im
Public Alias	test
Public User	eTGlobalUserName=Anonymous,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=Identity Manager,dc=etadb
Directory	IADBCorporate_Test
Provisioning Server	IADBProvisioning-Directory_Test
Install default roles	true
System Manager	IMAdmin (eTGlobalUserName=IMAdmin,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=Identity Manager,dc=etadb)
Policy Server Agent Group	hqdni06wa
Inbound Administrator	eTGlobalUserName=Inbound,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=Identity Manager,dc=etadb

<< Back Finish

Los ambientes y directorios se crean en réplica en SiteMinder políticas de servicio. Consulte la documentación de CA Identity Minder SiteMinder Integración

139

La consola de usuario de Identity Minder es una web basada en una interfaz de usuario que los administradores de Identity Minder utilizan para realizar tareas de administración.

Produccion Url:

http://newidm.iadb.org/iam/im/iadbprov/ca12/index.jsp

URL de Prueba:

http://idmt.iadb.org/ iam/im/provisioning-development/ca12/index.jsp

14.1.2 Directorio corporativo y el Directorio de abastecimiento

Proporcionar opciones para la gestión de usuarios y el abastecimiento automático de cuentas adicionales para aquellos usuarios , Identity Minder Coordena dos almacenes de usuarios :

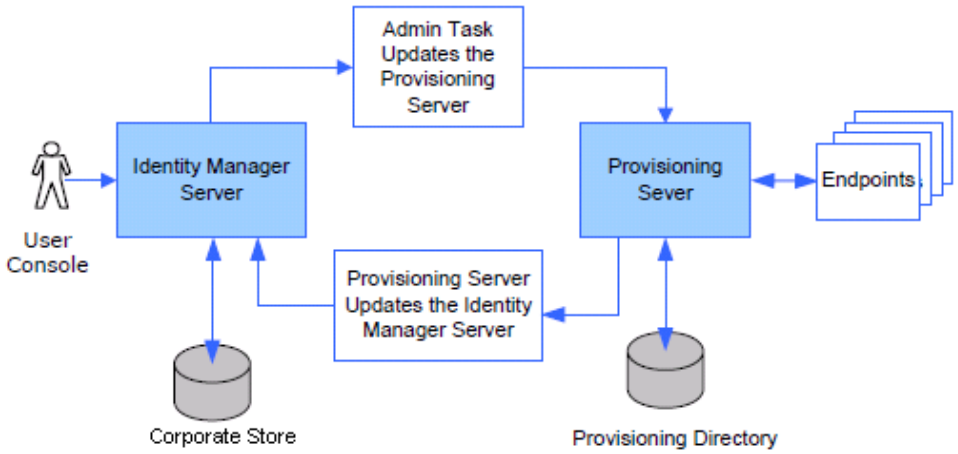
■ Directorio corporativo Identity Minder es el almacén de usuario mantenida por Identity Minder . Esta es una instancia de Directorio CA e incluye a los usuarios corporativos. En la Consola de administración , se crea un objeto del Directorio IdentityMinder para conectarse al almacén de usuario y describir los objetos de almacén de usuario que Identity Minder mantendrá .

■ Directorio de abastecimiento es el almacén de usuario mantenida por el servidor de abastecimiento . Es una instancia de directorio que incluye a los usuarios a nivel mundial , que se asocian a los usuarios en el Directorio de abastecimiento con cuentas en los endpoints, como Microsoft Exchange 2007 , Active Directory , Unix , Oracle y CA Access Control . Sólo algunos usuarios IdentityMinder tienen un usuario global correspondiente . Cuando un usuario Identity Minder recibe un papel de abastecimiento, el servidor de aprovisionamiento crea un usuario global . Los usuarios pueden ser asignados a uno o más roles de aprovisionamiento

La implementacio de Identity Minder utiliza directorios separados Directorio Corporativo y aprovisionamiento .

140

A continuación se muestra un ejemplo que demuestra cómo los cambios realizados en el servidor de mensajería instantánea / aprovisionamiento se propagan a los endpoints.



14.1.3 Extensiones de esquema Directorio

14.1.4 El esquema de Active Directory se extendió por el BID para apoyar los requisitos de directorio de Identity Minder para permitir atributos requeridos por mensajería instantanea. Algunos atributos son para la funcionalidad de autoservicio

Name	OID	Description	Syntax	Type	Object
smMarca	1.1.1.1	Atributo de Extencion - SiteMinder	Casos restringidos cadena	Univalue	Usuario
smDatos	1.1.1.2	Atributo de Extencion - SiteMinder	Octeto Cadena	?	Usuario
smRespuesta Desafio	1.1.1.3	Atributo de Extencion - SiteMinder	Codigo Cadena	Univalue	Usuario
smPregunta respuesta	1.1.1.4	Atributo de Extencion - SiteMinder	Codigo Cadena	Univalue	Usuario
SMAdminRoles	1.1.1.5	Atributo de Extencion - SiteMinderAdministration Roles	Codigo Cadena	Multivalue	Usuario

141

SMPWdatos	1.1.1.6	Atributo de Extencion - SiteMinderPassword Data	Codigo Cadena	Multivalue	Usuario
SMIdentyPoliticas	1.1.1.7	Atributo de Extencion - SiteMinderIdentity Policy	Codigo Cadena	Multivalue	Usuario
SMGrupoAdmin	1.1.1.8	Atributo de Extencion - SiteMinderGroup Administration	Unicode String	Multivalue	Grupo
SMAutomarcasubscripción	1.1.1.9	Atributo de Extencion - SiteMinder Self-Subscribing Flag	Unicode String	Univalue	Grupo
SMGrupoDinamicoQ	1.1.1.10	Atributo de Extencion - SiteMinderDynamic Group Q	Unicode String	Multivalue	Grupo
SMGrupo Aninado Nem	1.1.1.11	Atributo de Extencion - SiteMinderNested Group Membership	Unicode String	Multivalue	Grupo
SMAdminGrupoAdm	1.1.1.12	Atributo de Extencion - SiteMinderAdmin Group Administration	Unicode String	Multivalue	Grupo

14.1.5 Base de datos Identity Minder

Esta base de datos contiene información de configuración de Identity Minder, información sobre las actividades de Identity Minder y sus eventos asociados con el tiempo, y un registro histórico de las operaciones que tienen lugar en el entorno de Identity Minder.

Hay 5 casos DB en el clúster de servidores MS SQL : Auditoría , Tarea Persistencia , Objetos , informes y flujos de trabajo .

Pruebas IDM DBs:

1. IM Base de datos de almacen de objetos.

Nombre de base de datos - IDM_DBDEVN

Puerto – 2974

Hospedaje- IDBTRDA1\IDBTRDA1INST1

2. Base de datos de reporte de instantaneas

Base de datos nombre: - IDM_REPDEVN

Puerto – 2974

142

Hospedaje - IDBTRDA1\IDBTRDA1INST1

Prod IDM DBs

1. IM Base de datos de almacen de objetos

Nombre base de datos - IDM_DBPRODN

Puerto – 2974

Hospedaje - IDBPRDA1\IDBPRDA1INST1

2. Informe de la base de datos de instantanea

Nombre de base de datos - IDM_REPDEVN

Puerto– 2974

Hospedaje - IDBPRDA1\IDBPRDA1INST1

14.1.6 Provisioning Server (Anteriormente eTrust Admin)

El Provisioning Server es el servidor que maneja las cuentas adicionales que se asignan a un usuario Identity Minder . Al asignar un rol de aprovisionamiento a un usuario Identity Minder , el servidor de aprovisionamiento crea cuentas en los endpoints que cumplan con los requisitos de la función . Por ejemplo , si asigna un rol de aprovisionamiento que incluye una plantilla de cuenta de Exchange , el servidor de aprovisionamiento asigna una cuenta de Exchange para el usuario.

El servidor de aprovisionamiento se administra a través de una herramienta de interfaz gráfica - Provisioning Manager.

Esto se utiliza para tareas administrativas, tales como la adquisición de criterios de valoración , la instalación de tipos de punto final , y la gestión de opción de servidor de aprovisionamiento

143

15 ENTORNO SITEMINDER

15.1.1 Hospedaje(ver tabla 37)

Tabla 37 – Hospedaje

ENTORNO	COMPONENTES	NOMBRE DE HOSPEDAJE
Prueba		
	SERVIDOR WEB	hqdni06
	POLITICAS DE SERVIDOR	hqtasmidm01
	ADMIN UI	hqtasmidm02
PROD		
	SERVIDOR WEB 1	hqpniweb07
	POLITICAS DE SERVIDOR 1	hqpasmidm02
	ADMIN UI1	hqpasmidmui01
	SERVIDOR WEB2	hqpniweb08
	POLITICAS DE SERVIDOR 2	hqpasmidm02
	ADMIN UI2	hqpasmidmui02

15.1.2 Admin URLs(ver tabla 38)

Tabla 38 – Admin URLs

PROD1 Admin UI	https://hqpasmidmui01.idb.iadb.org:8443/iam/siteminder/console/
PROD2 Admin UI	https://hqpasmidmui02.idb.iadb.org:8443/iam/siteminder/console/
TEST Admin UI	https://hqtasmidm02.idb.iadb.org:8443/iam/siteminder/console/ca12/index.jsp

144

15.1.3 ACCESO A SiteMinder

Forma alternativa de acceder a Siteminder administración en v12.5 SM

http://hqpasmidm01/siteminder/smadmin2.html

15.1.4 Base de datos SiteMinder

SiteMinder necesita una base de datos (también puede ser un LDAP compatible) para Policy Store y almacén de cla ves. Actualmente BID utiliza MS SQL Server para las tiendas de política.

Prod: idbprda2\idbprda2inst2\SMIDMPRD

Test: idbtrda2\idbtrda2inst2\SMIDMDBTST

15.1.5 SiteMinder Policy Server

Proporciona autenticación avanzada de Identidad Minder , y proporciona acceso a las funciones SiteMinder , como contraseña Servicios y Single Sign -On .

Actualmente la autenticación está configurado para ser manejado por SiteMinder y autorización está a cargo de Identidad Minder . Véase el documento CA Identity Minder SiteMinder Integración .

15.1.6 Los URLs de IdentityMinder se encuentran protegidos por Siteminder

15.1.6.1 Pruebas

https://idmt.idb.iadb.org/iam/immanage/

https://hdni06.idb.iadb.org/iam/immanage/

https://idmt.idb.iadb.org/iam/im/provisioning-development

https://hqdni06.idb.iadb.org/iam/im/provisioning-development

15.1.6.2 PRODUCCIÓN

http://hqpniweb07.idb.iadb.org/iam/immanage

http://hqpniweb08.idb.iadb.org/iam/immanage

http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/

http://hqpniweb08.idb.iadb.org/iam/im/iadbprov/

146

16 IAM Servidor de informes

(Note: Por favor vea documentos SIS para mas deralles de instalación y pasos de configuración de informes del servidor.)

Identity Minder proporciona informes que se pueden utilizar para controlar el estado de un entorno Identidad Minder . IAM servidor de informes es impulsado por Business Objects Enterprise XI .

Produccion Url:

http://hqpacorpn:8080/InfoView/logon.jsp

Url de prueba:

http://hqdacorpn:8080/InfoView/logon.jsp

16.1.1 Los informes se accede mediante Business Objects credenciales. Vea el archivo principal, una hoja de Excel separada mantenida por el BID para los nombres de usuario y contraseñas

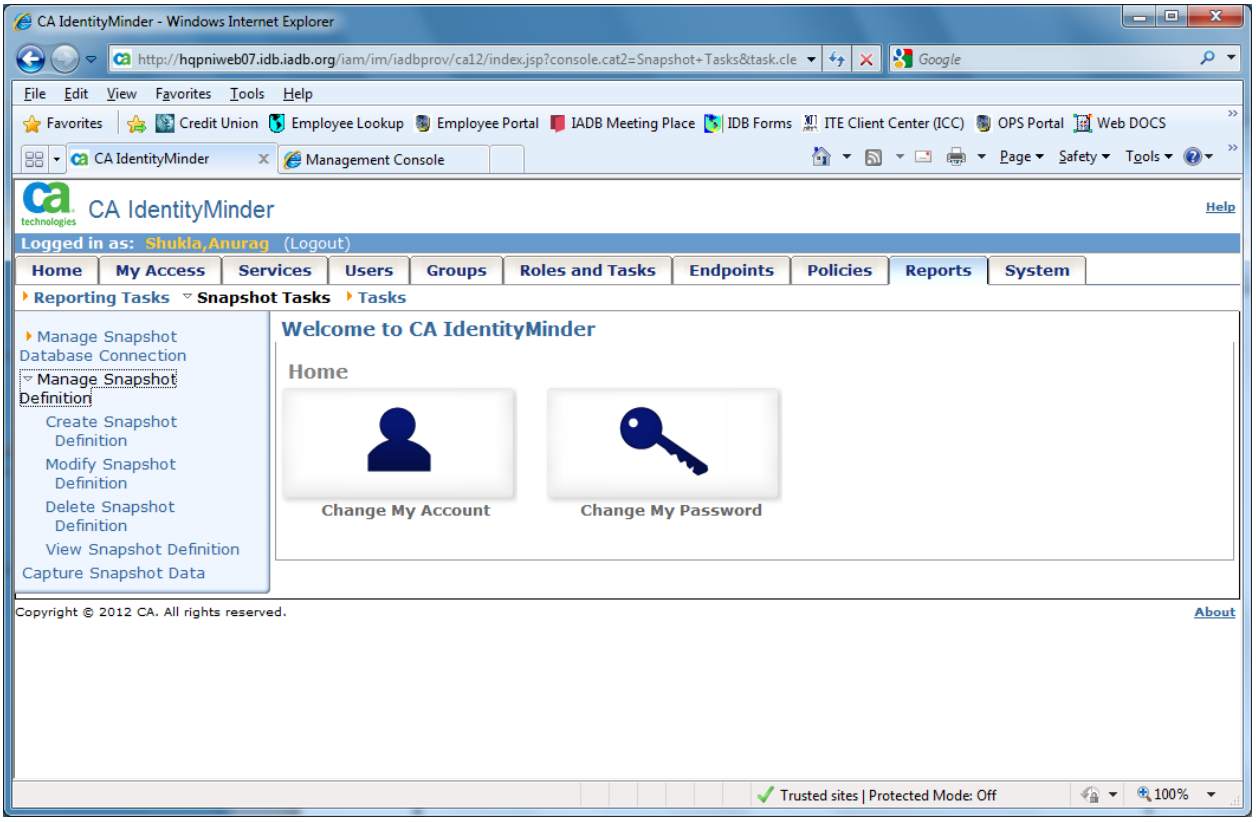
16.1.2 Base de datos de informes

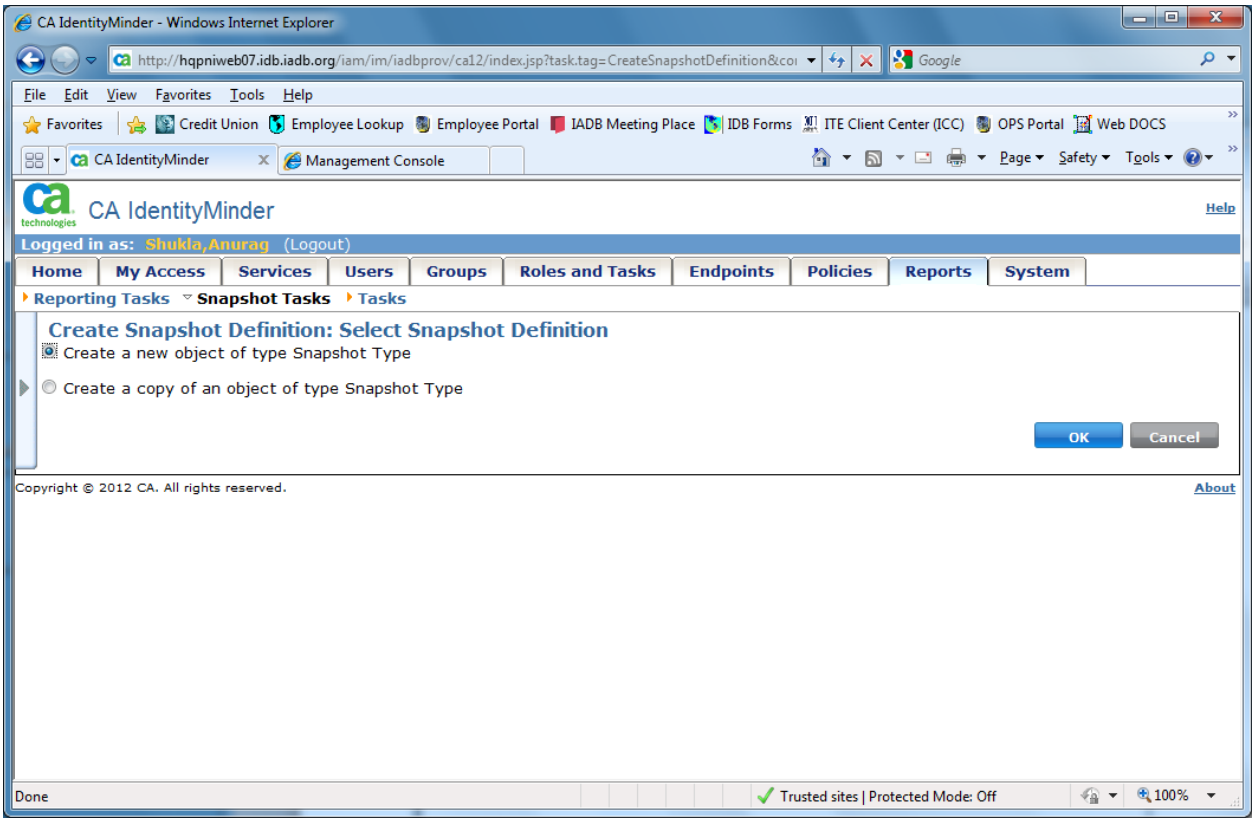
Tiendas instantánea de datos , lo que refleja el estado actual de los objetos en Identity Minder en el momento en que se toma la instantánea. Los informes se generan a partir de esta información para ver la relación entre objetos, como usuarios y roles .

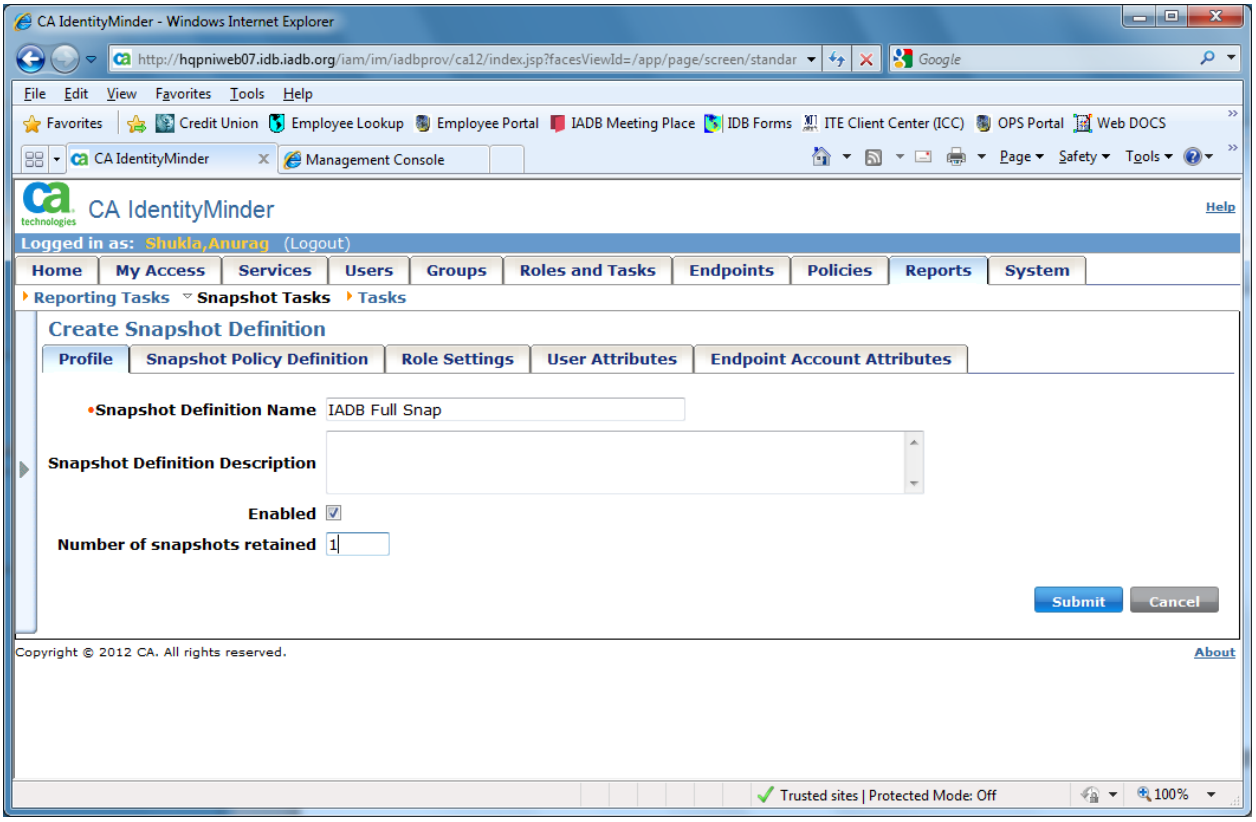
16.1.3 Definición de crear instantanea

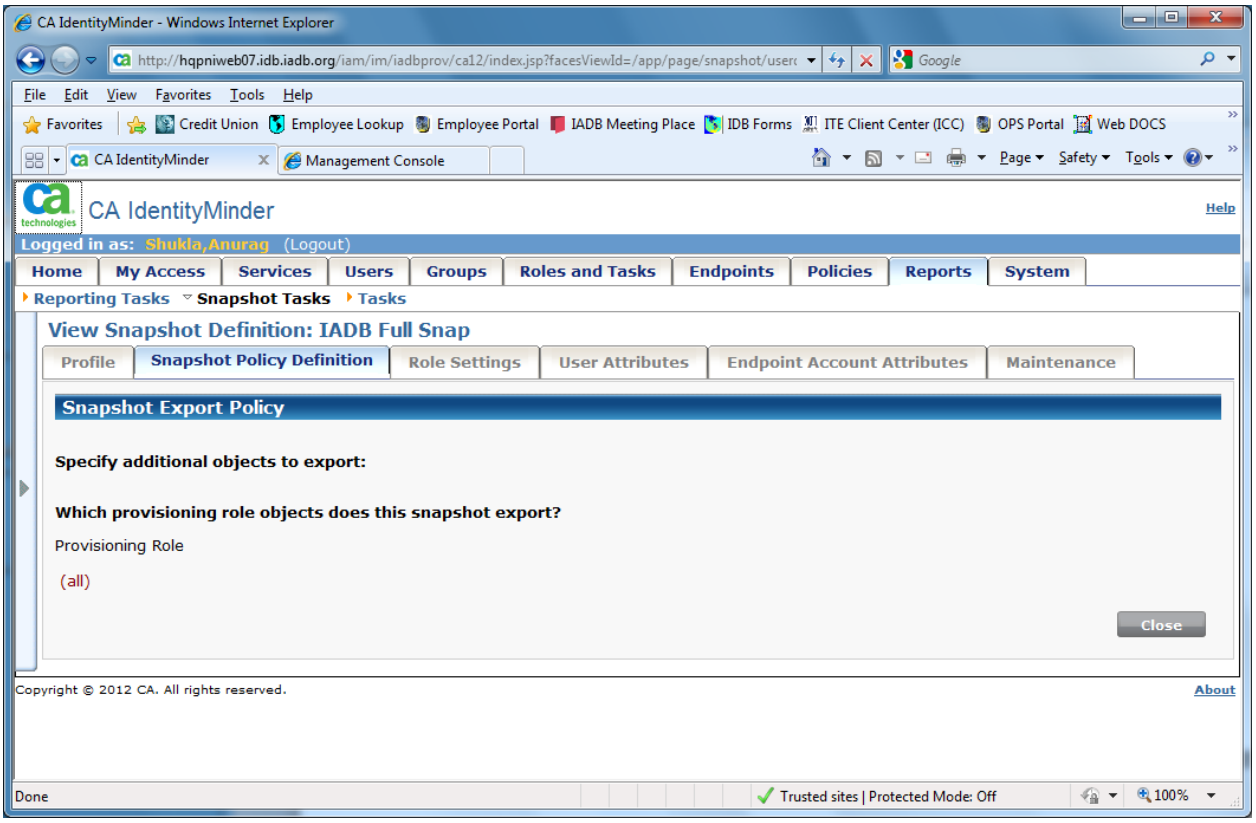
Ingresa a la consola de Identity Minder

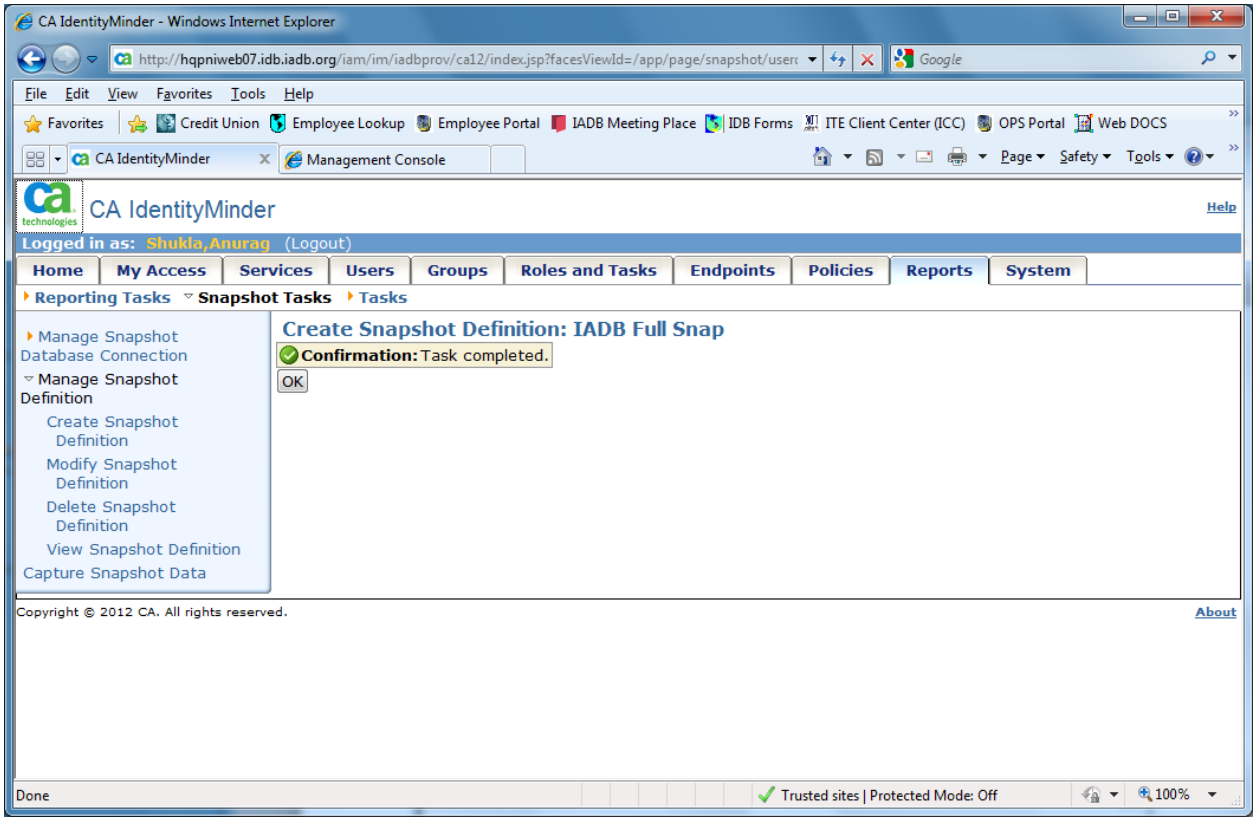
147

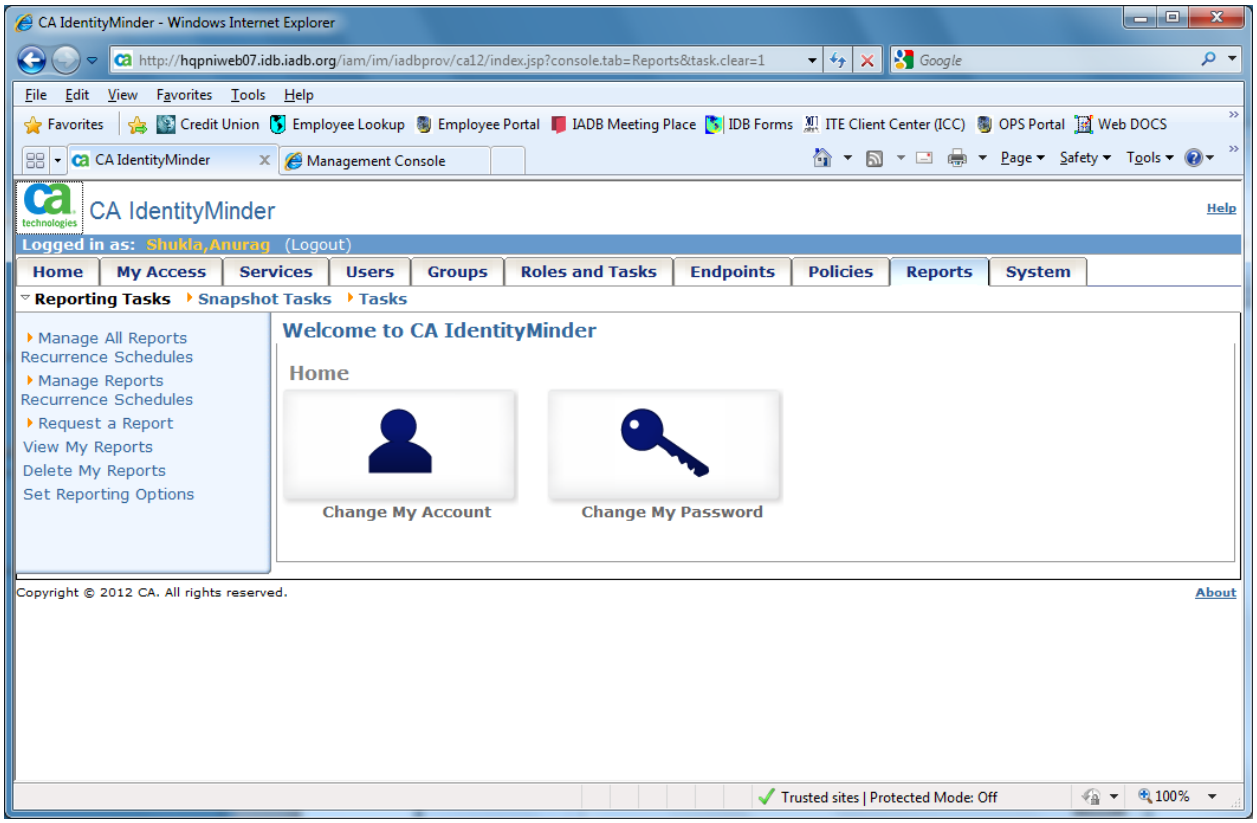

CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?console.cat2=Snapshot+Tasks&task.cle
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Manage Snapshot Database Connection
Manage Snapshot Definition
Create Snapshot Definition
Modify Snapshot Definition
Delete Snapshot Definition
View Snapshot Definition
Capture Snapshot Data
Welcome to CA IdentityMinder
Home
Change My Account
Change My Password
Copyright © 2012 CA. All rights reserved.
About
Trusted sites | Protected Mode: Off
100%

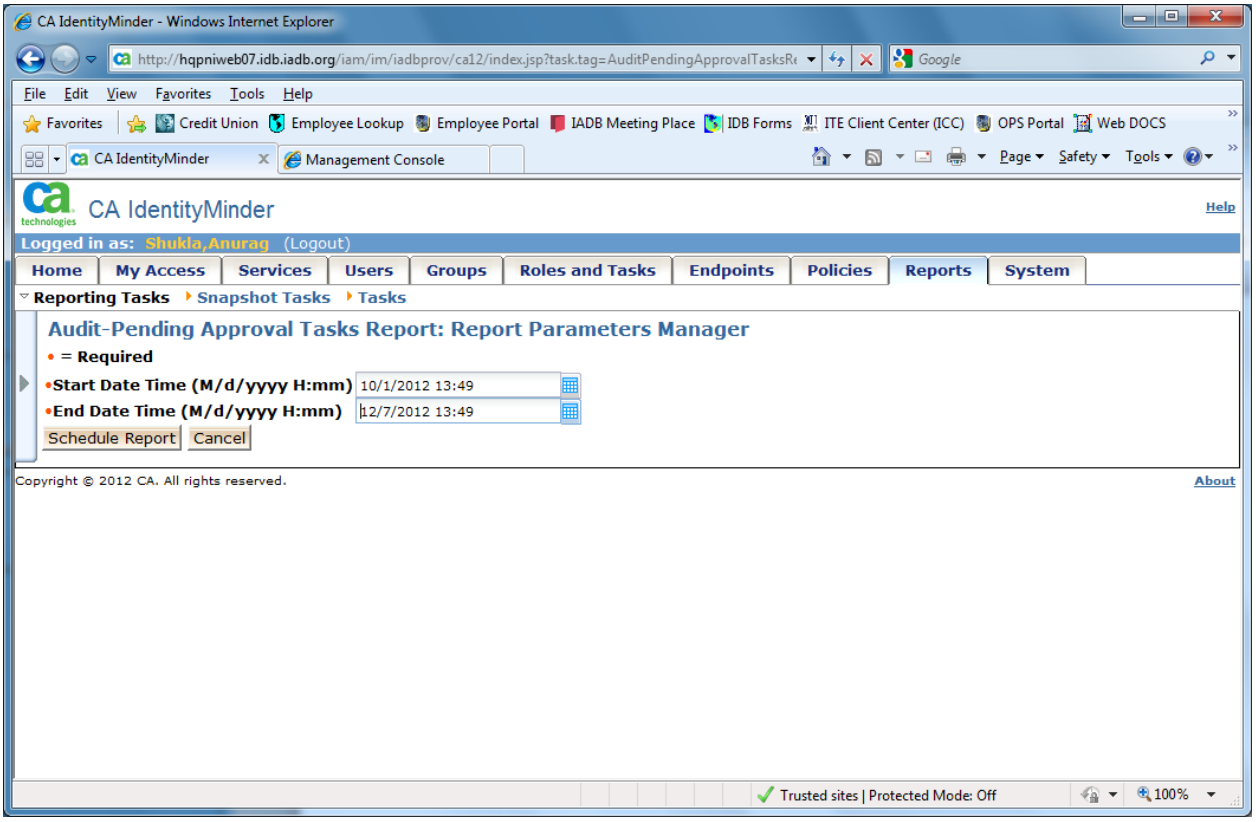

CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?task.tag=CreateSnapshotDefinition&co
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Create Snapshot Definition: Select Snapshot Definition
Create a new object of type Snapshot Type
Create a copy of an object of type Snapshot Type
OK
Cancel
Copyright © 2012 CA. All rights reserved.
About
Done
Trusted sites | Protected Mode: Off
100%

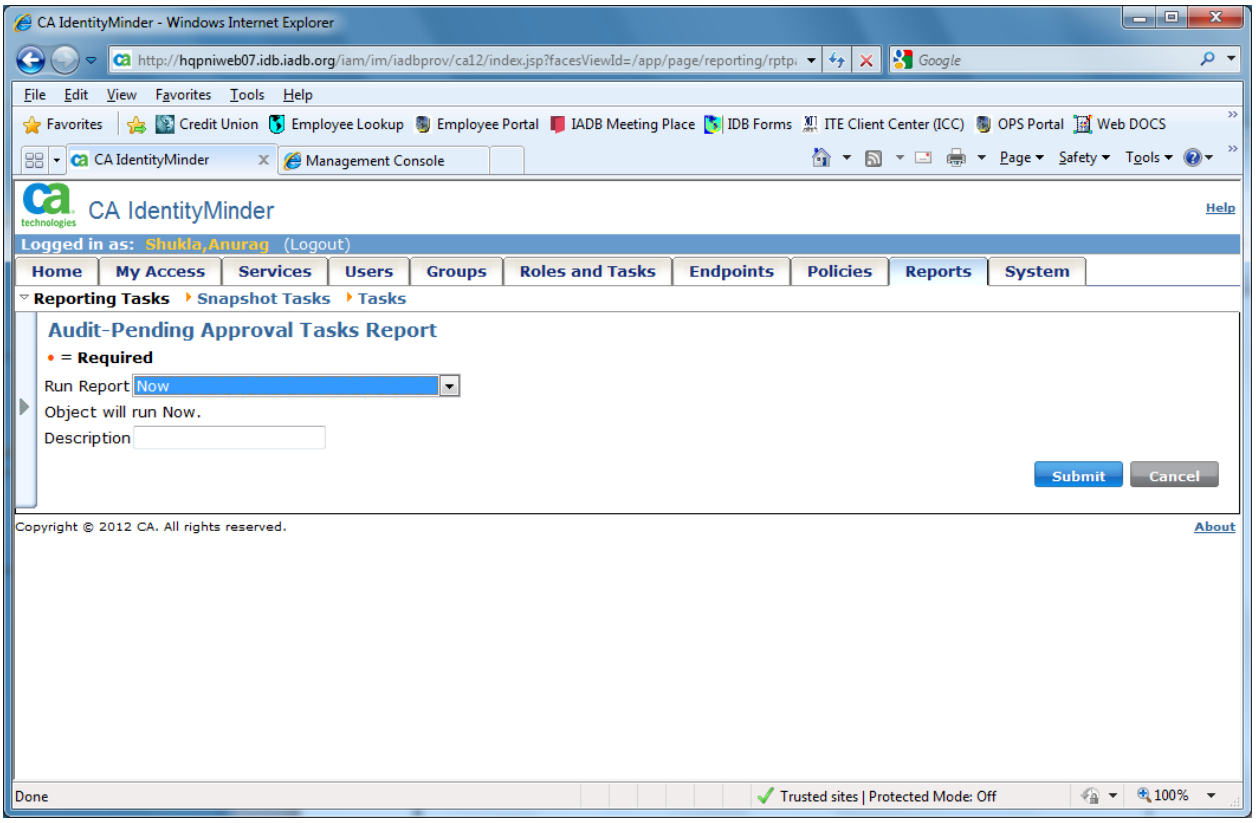

CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/screen/standar
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Create Snapshot Definition
Profile Snapshot Policy Definition Role Settings User Attributes Endpoint Account Attributes
Snapshot Definition Name IADB Full Snap
Snapshot Definition Description
Enabled
Number of snapshots retained 1
Submit Cancel
Copyright © 2012 CA. All rights reserved.
About
Trusted sites | Protected Mode: Off
100%

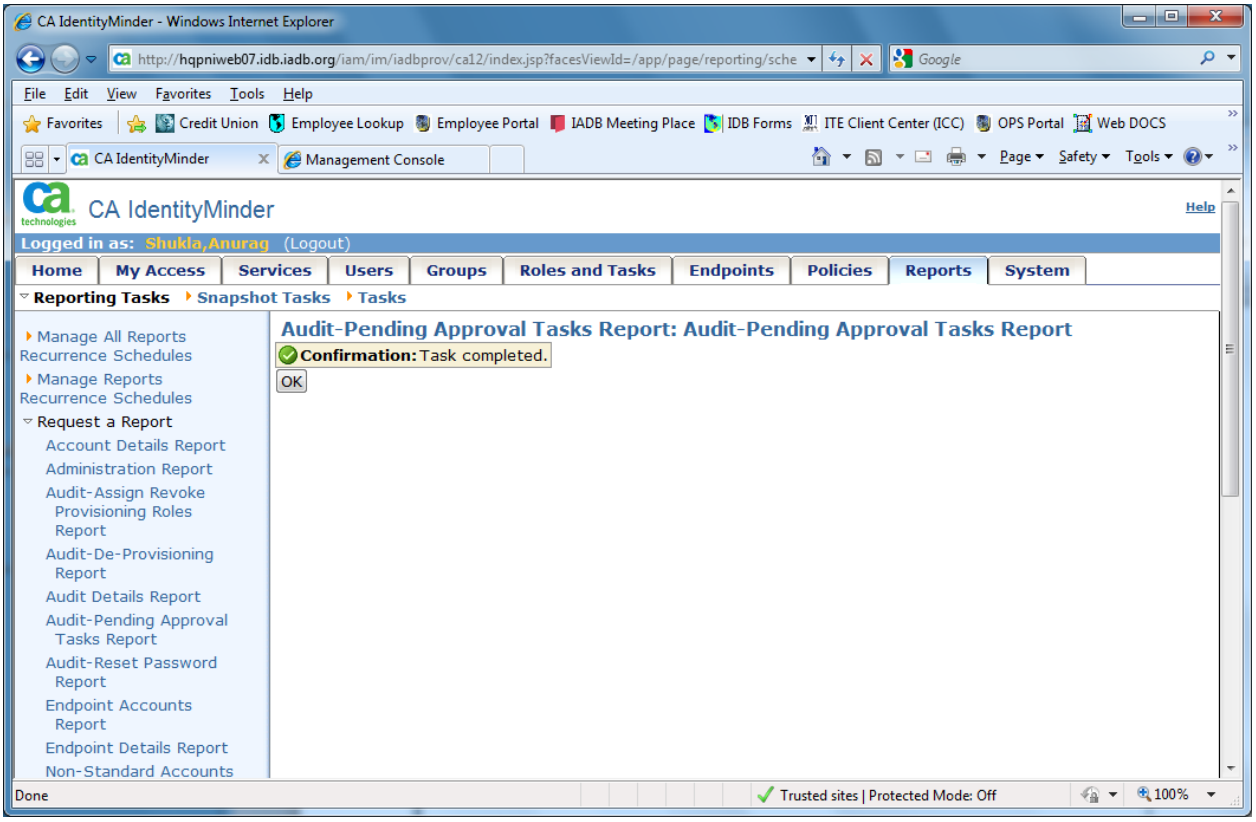

CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/snapshot/user
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
View Snapshot Definition: IADB Full Snap
Profile Snapshot Policy Definition Role Settings User Attributes Endpoint Account Attributes Maintenance
Snapshot Export Policy
Specify additional objects to export:
Which provisioning role objects does this snapshot export?
Provisioning Role
(all)
Close
Copyright © 2012 CA. All rights reserved.
About
Done
Trusted sites | Protected Mode: Off
100%

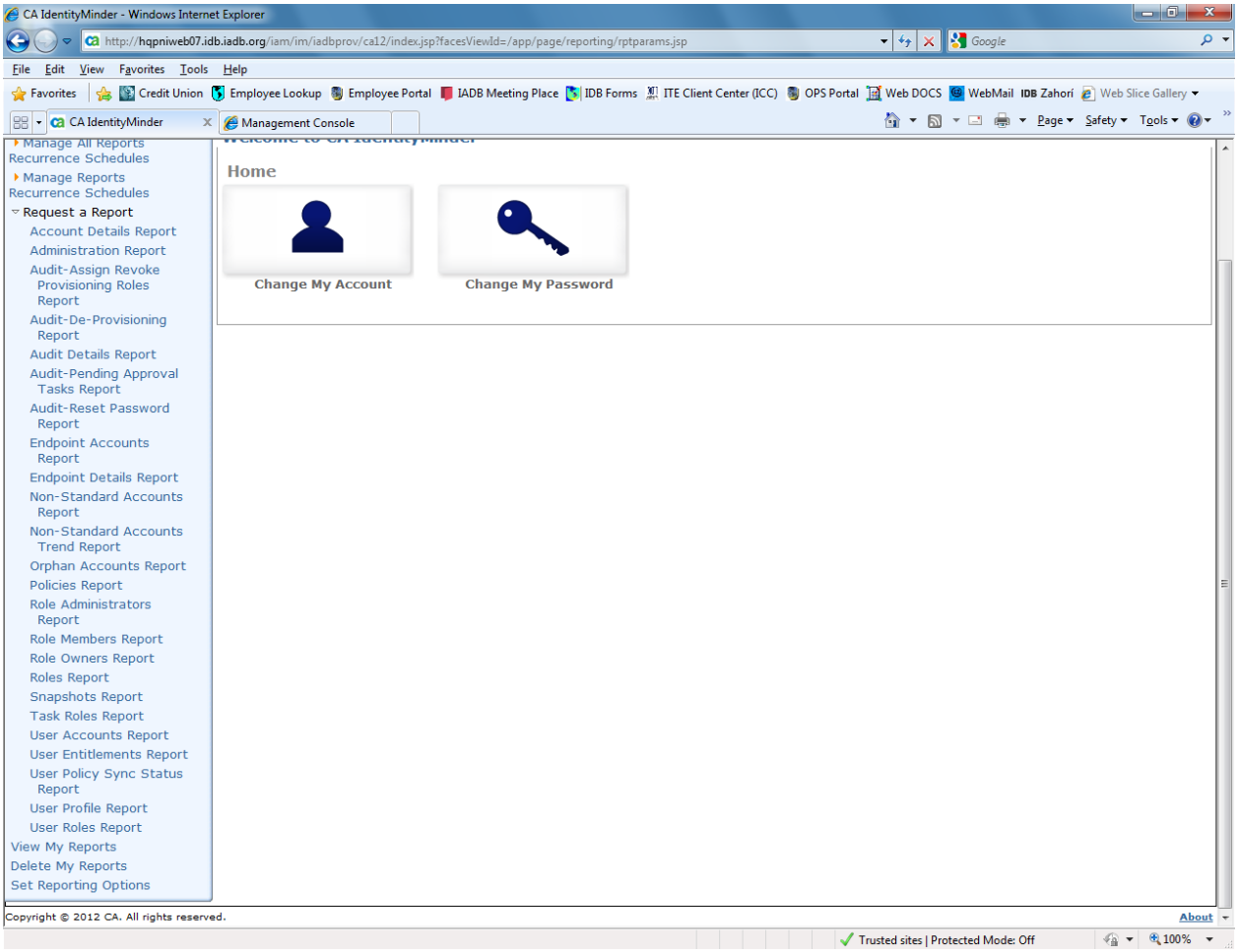

CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/snapshot/user
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
Page Safety Tools
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Manage Snapshot Database Connection
Manage Snapshot Definition
Create Snapshot Definition
Modify Snapshot Definition
Delete Snapshot Definition
View Snapshot Definition
Capture Snapshot Data
Create Snapshot Definition: IADB Full Snap
Confirmation: Task completed.
OK
Copyright © 2012 CA. All rights reserved.
About
Done
Trusted sites | Protected Mode: Off
100%

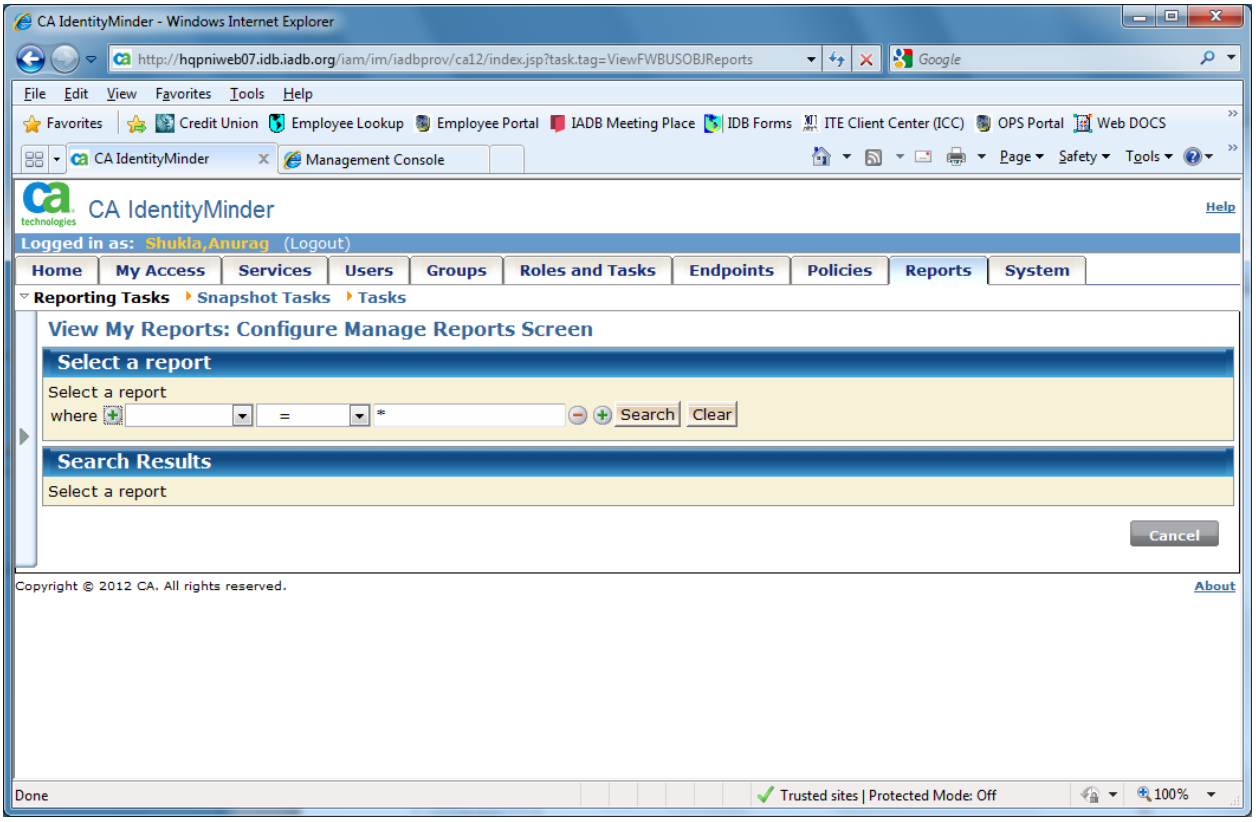

CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?console.tab=Reports&task.clear=1
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
Page Safety Tools
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Manage All Reports Recurrence Schedules
Manage Reports Recurrence Schedules
Request a Report
View My Reports
Delete My Reports
Set Reporting Options
Welcome to CA IdentityMinder
Home
Change My Account
Change My Password
Copyright © 2012 CA. All rights reserved.
About
Trusted sites | Protected Mode: Off
100%


CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?task.tag=AuditPendingApprovalTasksR
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Audit-Pending Approval Tasks Report: Report Parameters Manager
• = Required
•Start Date Time (M/d/yyyy H:mm) 10/1/2012 13:49
•End Date Time (M/d/yyyy H:mm) 12/7/2012 13:49
Schedule Report Cancel
Copyright © 2012 CA. All rights reserved.
About
Trusted sites | Protected Mode: Off
100%


CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/reporting/rptp
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Audit-Pending Approval Tasks Report
• = Required
Run Report Now
Object will run Now.
Description
Submit Cancel
Copyright © 2012 CA. All rights reserved.
About
Done
Trusted sites | Protected Mode: Off
100%


CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/reporting/sche
Google
File Edit View Favorites Tools Help
Favorites Credit Union Employee Lookup Employee Portal IADB Meeting Place IDB Forms ITE Client Center (ICC) OPS Portal Web DOCS
CA IdentityMinder
Management Console
Page Safety Tools
CA IdentityMinder
Help
Logged in as: Shukla,Anurag (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Reporting Tasks Snapshot Tasks Tasks
Manage All Reports Recurrence Schedules
Manage Reports Recurrence Schedules
Request a Report
Account Details Report
Administration Report
Audit-Assign Revoke Provisioning Roles Report
Audit-De-Provisioning Report
Audit Details Report
Audit-Pending Approval Tasks Report
Audit-Reset Password Report
Endpoint Accounts Report
Endpoint Details Report
Non-Standard Accounts
Audit-Pending Approval Tasks Report: Audit-Pending Approval Tasks Report
Confirmation: Task completed.
OK
Done
Trusted sites | Protected Mode: Off
100%


CA IdentityMinder - Windows Internet Explorer
http://hqpniweb07.idb.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/reporting/rptparams.jsp
File Edit View Favorites Tools Help
Favorites
Credit Union
Employee Lookup
Employee Portal
IADB Meeting Place
IDB Forms
ITE Client Center (ICC)
OPS Portal
Web DOCS
WebMail
IDB Zahorí
Web Slice Gallery
CA IdentityMinder
Management Console
Page
Safety
Tools
Manage All Reports
Recurrence Schedules
Manage Reports
Recurrence Schedules
Request a Report
Account Details Report
Administration Report
Audit-Assign Revoke Provisioning Roles Report
Audit-De-Provisioning Report
Audit Details Report
Audit-Pending Approval Tasks Report
Audit-Reset Password Report
Endpoint Accounts Report
Endpoint Details Report
Non-Standard Accounts Report
Non-Standard Accounts Trend Report
Orphan Accounts Report
Policies Report
Role Administrators Report
Role Members Report
Role Owners Report
Roles Report
Snapshots Report
Task Roles Report
User Accounts Report
User Entitlements Report
User Policy Sync Status Report
User Profile Report
User Roles Report
View My Reports
Delete My Reports
Set Reporting Options
Home
Change My Account
Change My Password
Copyright © 2012 CA. All rights reserved.
About
Trusted sites | Protected Mode: Off
100%

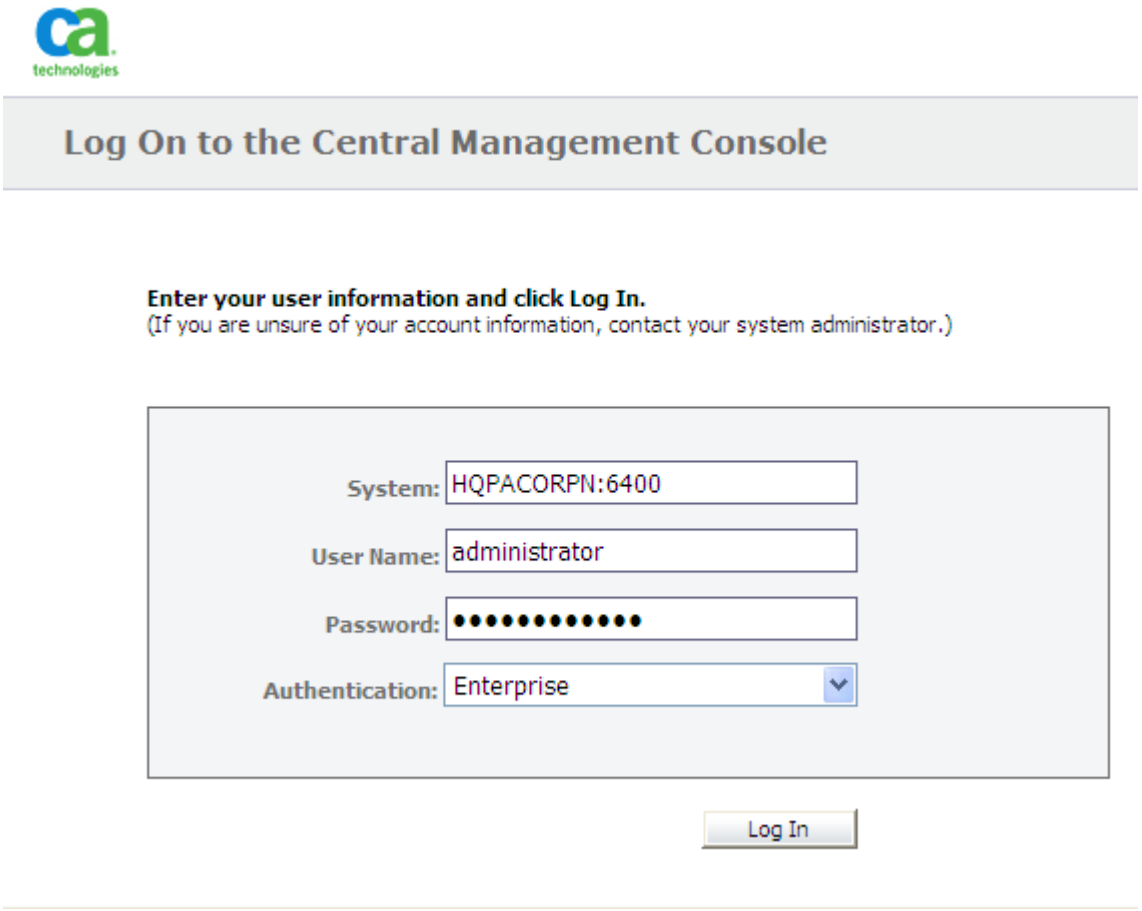


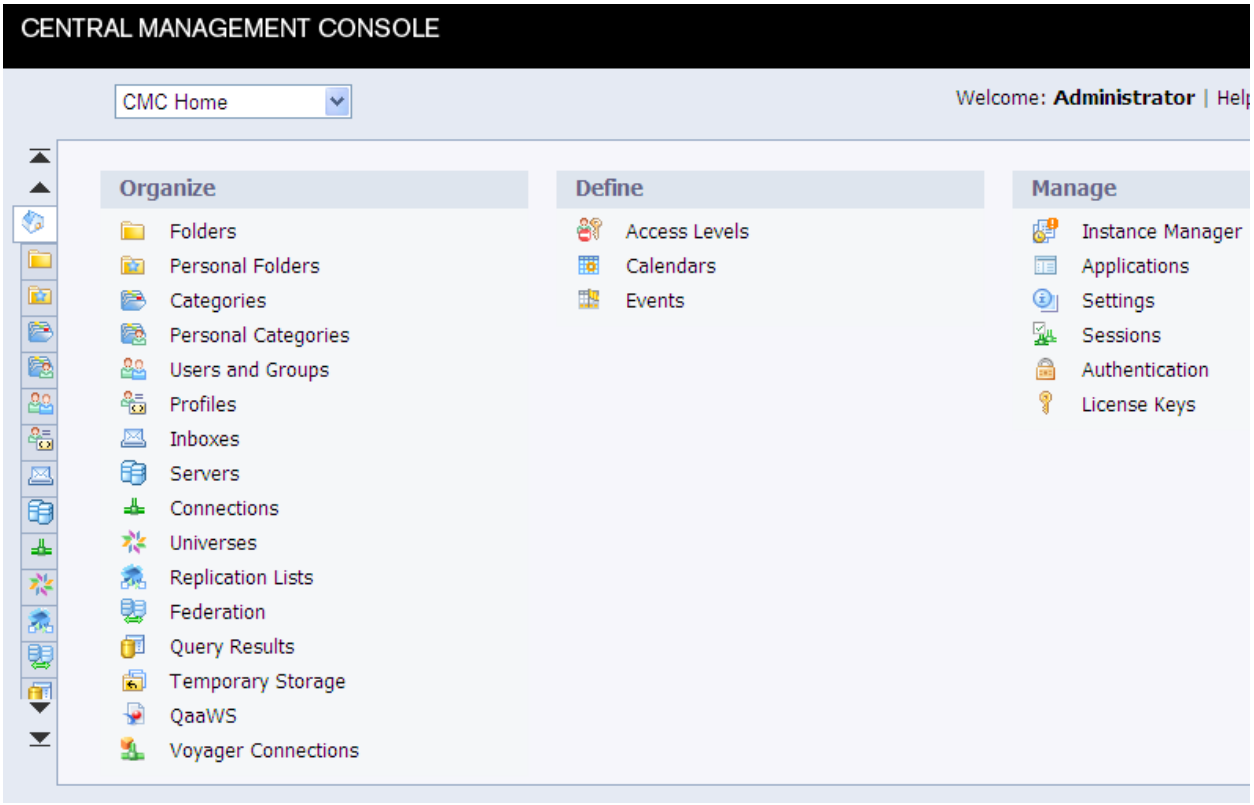
Los informes son visibles directamente regístrandose para la consola de administración central de Business Objects. Después de ejecutar el informe de la consola de usuario de mensajería instantánea , abra el siguiente enlace:

Launchpad Url :

http://hqpacorpn:8080/CmcApp/logon.faces

Inicie Consola de administración central > registrado como administrador- > carpetas > MI informes-> seleccionar un informe- > Historia-> haga clic en la instancia de informe


Log On to the Central Management Console
Enter your user information and click Log In.
(If you are unsure of your account information, contact your system administrator.)
System:
HQPACORPN:6400
User Name:
administrator
Password:
Authentication:
Enterprise
Log In


CENTRAL MANAGEMENT CONSOLE
CMC Home
Welcome: Administrator | Hel
Organize
Folders
Personal Folders
Categories
Personal Categories
Users and Groups
Profiles
Inboxes
Servers
Connections
Universes
Replication Lists
Federation
Query Results
Temporary Storage
QaaWS
Voyager Connections
Define
Access Levels
Calendars
Events
Manage
Instance Manager
Applications
Settings
Sessions
Authentication
License Keys

156

17 Tareas administrativas personalizadas de Identity Manager

Las siguientes tareas de administración personalizados se crearon para cubrir todos los casos de uso

.Añadir BID usuario

• Transferencia BID usuario

• Terminar BID usuario

• recontratación BID usuario

• Aprovisionamiento Crear usuario

• Aprovisionamiento Modificar usuario

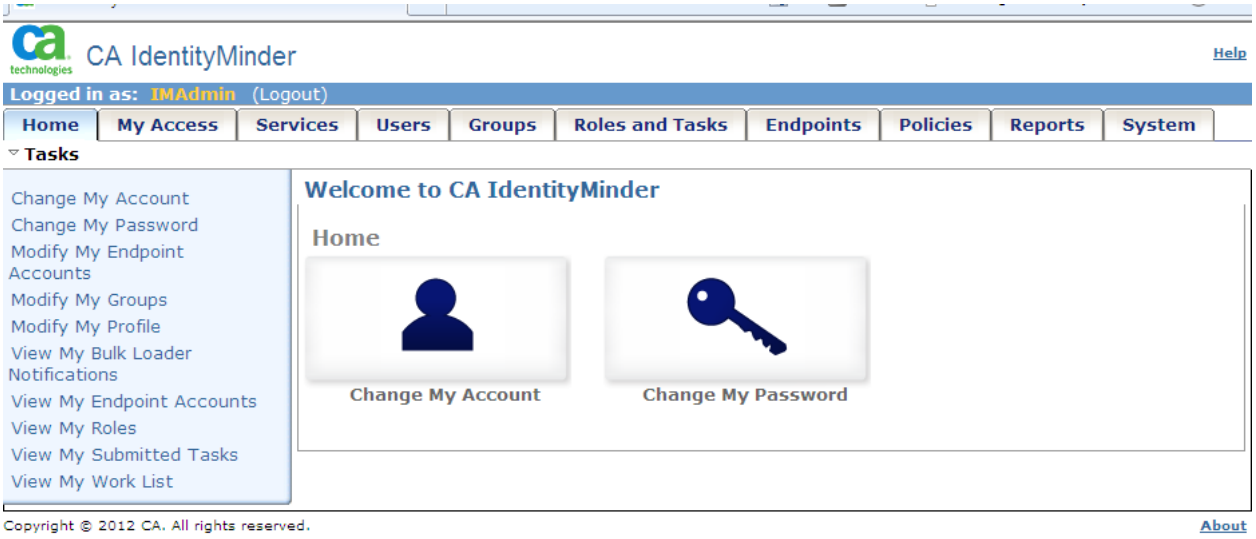
17.1 Agregar IADB Usuario

Utilice esta tarea para crear un nuevo usuario de Identity Manager . Con el fin de crear cuentas en los endpoints, asignar roles de aprovisionamiento para el usuario.

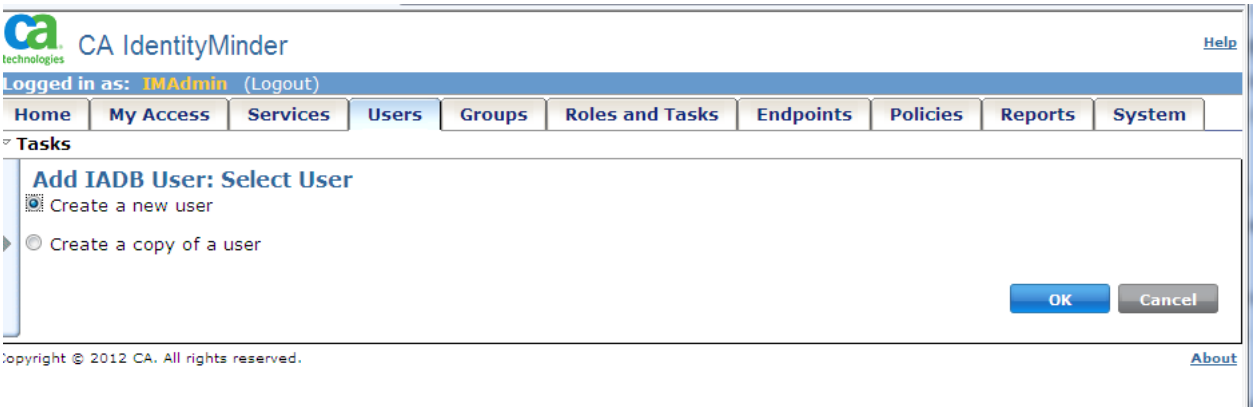
Notificación por correo electrónico se envía en la realización de tareas ' Añadir BID usuario , es decir después de una exitosa creación de usuario de mensajería instantánea, sin tener en cuenta si no se añaden funciones de aprovisionamiento para las cuentas de punto final.

Notificaciones de correo electrónico no están habilitadas para el nativo ' Modificar usuario de tareas, para evitar el envío de notificaciones por ejemplo , cuando se cambia un número de teléfono . Por lo tanto, si se agrega / eliminar usuario aprovisionamiento papeles utilizando ' Modificar usuario , no se enviarán notificaciones por correo electrónico .

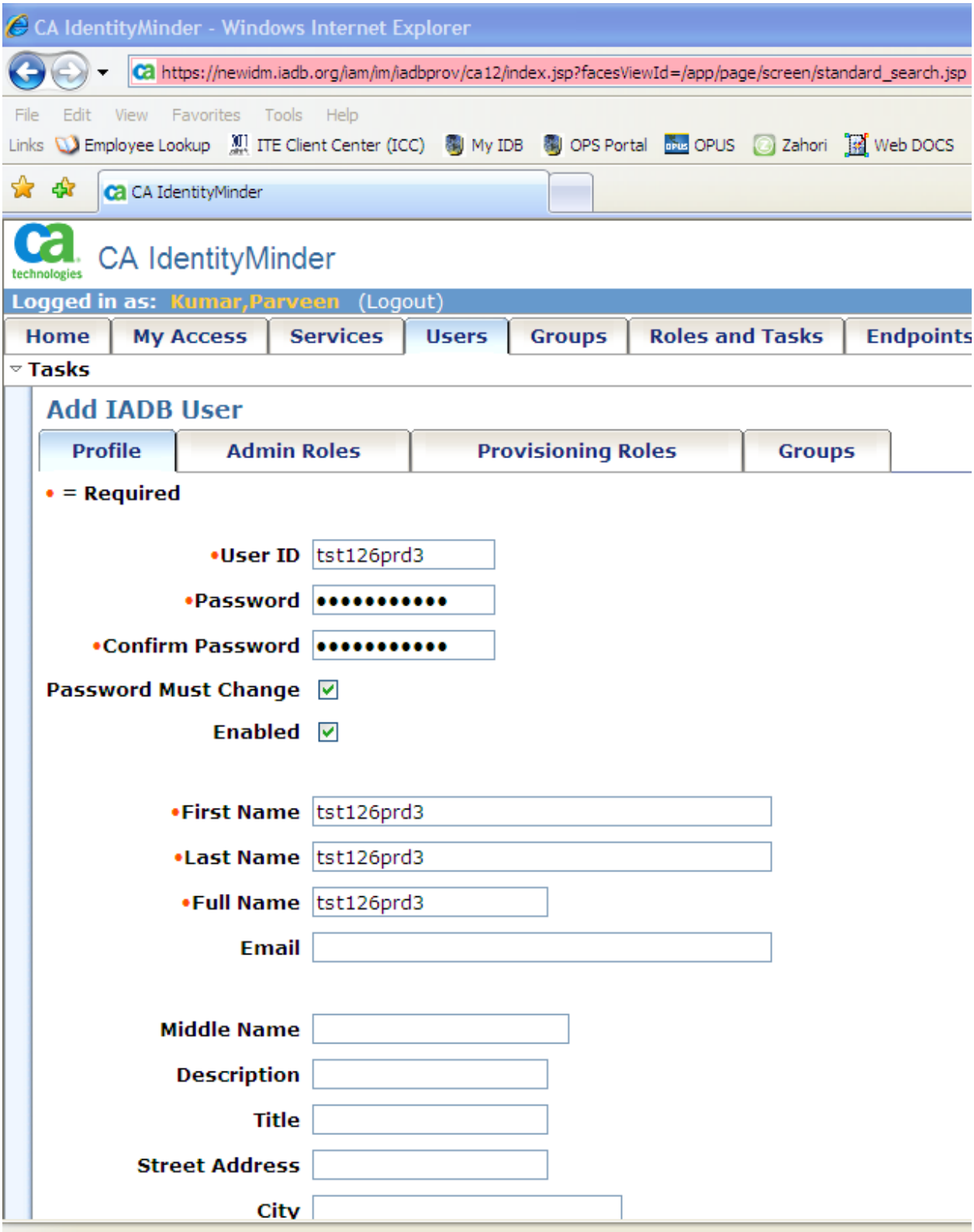
Inicia sesión para Identity Manager consola de usuario como administrador.

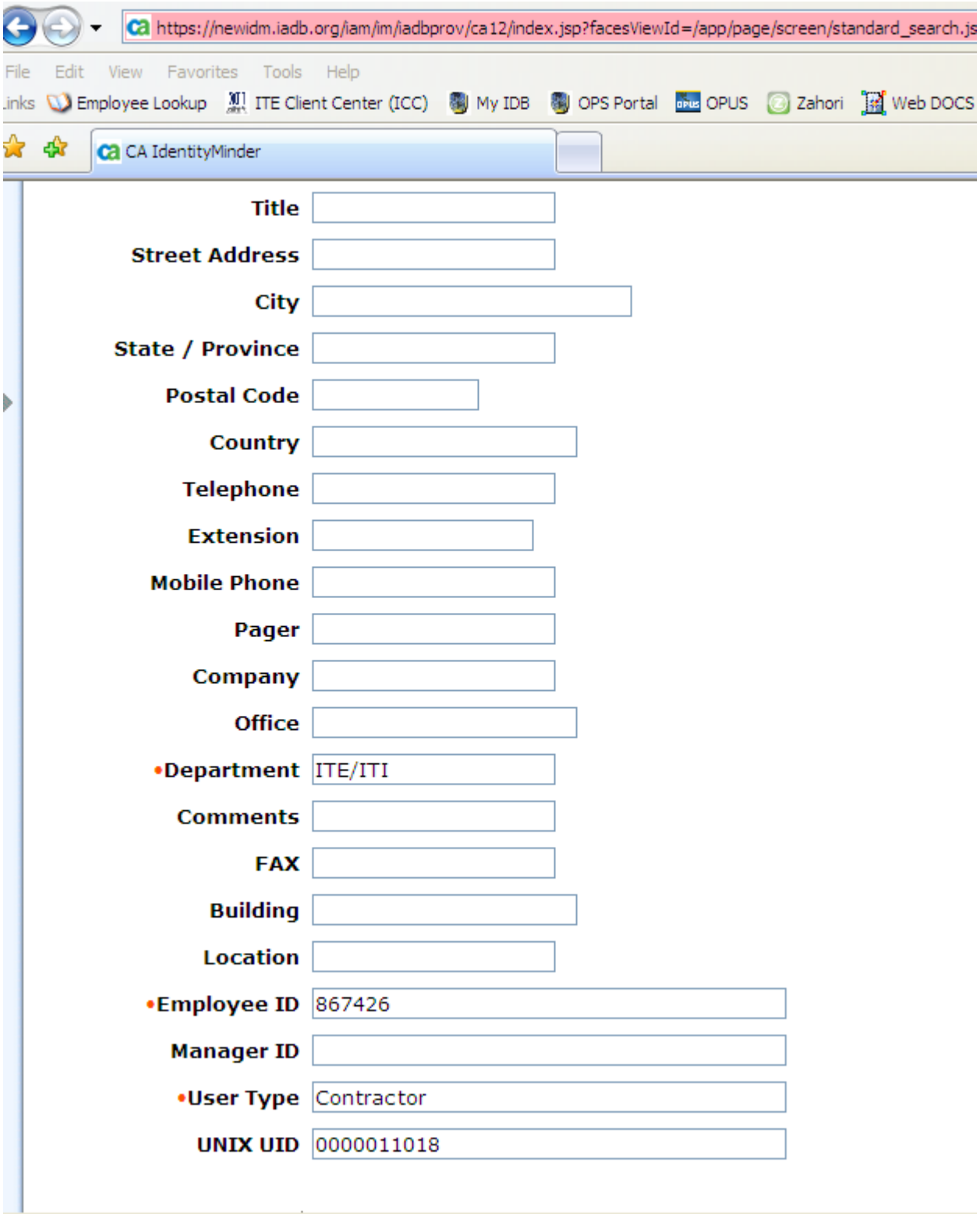


Busque Usuarios- > Administrar usuarios- > Añadir BID usuario

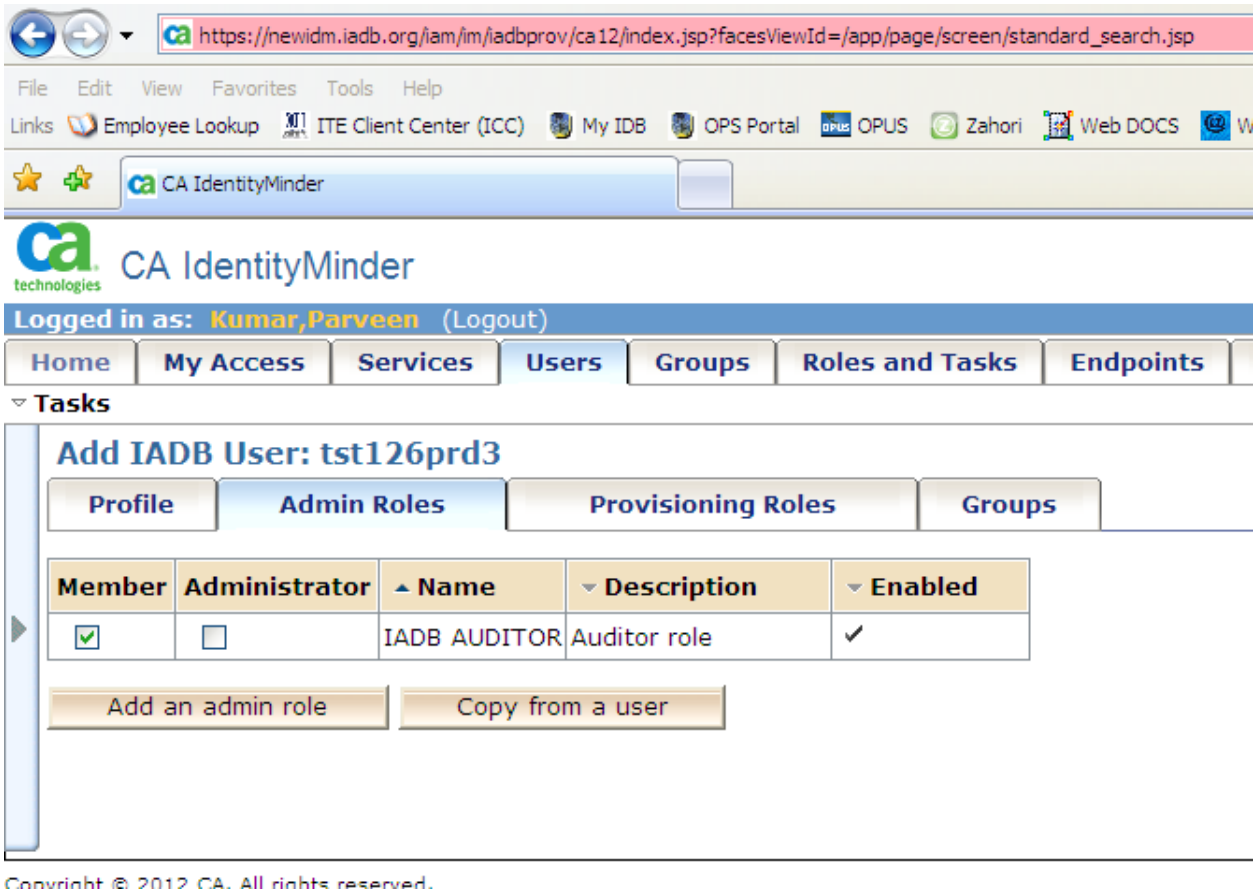


Rellene el formulario de usuario nuevo

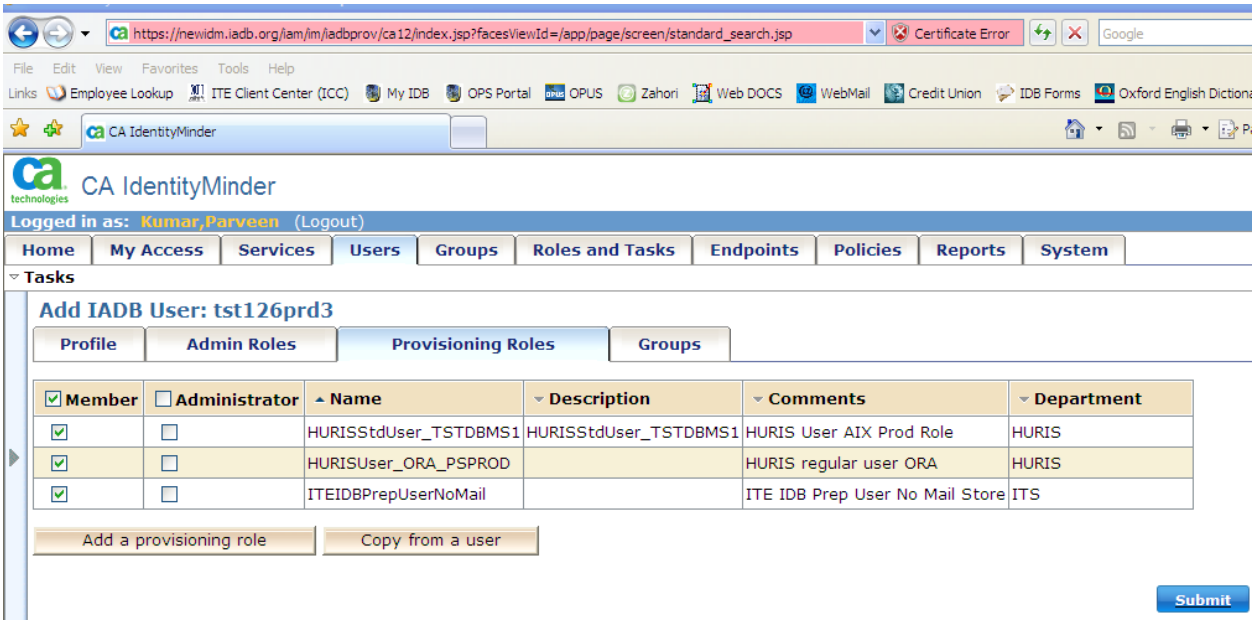

CA IdentityMinder - Windows Internet Explorer
https://newidm.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/screen/standard_search.jsp
File Edit View Favorites Tools Help
Links Employee Lookup ITE Client Center (ICC) My IDB OPS Portal OPUS Zahori Web DOCS
CA IdentityMinder
CA IdentityMinder
Logged in as: Kumar,Parveen (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints
Tasks
Add IADB User
Profile Admin Roles Provisioning Roles Groups
• = Required
•User ID tst126prd3
•Password ••••••••••
•Confirm Password ••••••••••
Password Must Change
Enabled
•First Name tst126prd3
•Last Name tst126prd3
•Full Name tst126prd3
Email
Middle Name
Description
Title
Street Address
City



Haga clic en los roles de administrador para agregar rol de administrador (s)

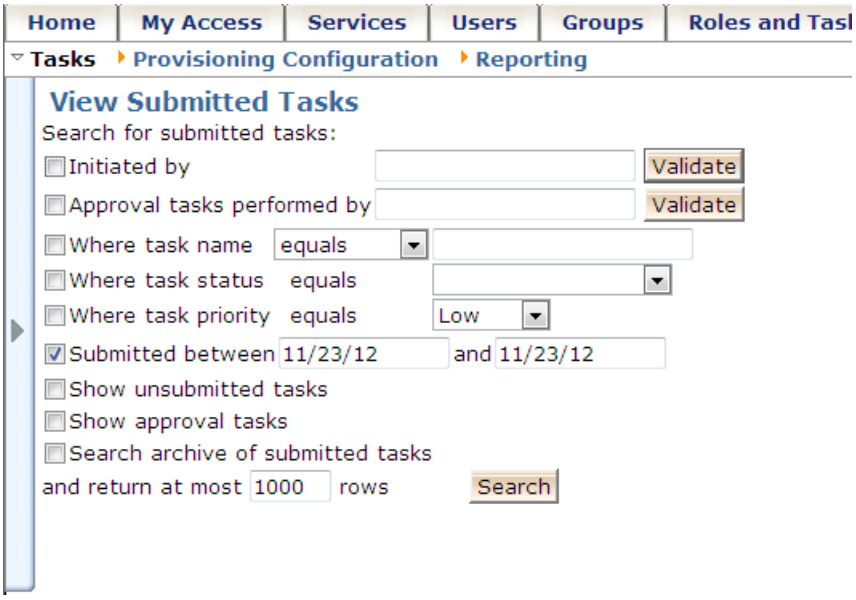


Haga clic sobre la función (s) de aprovisionamiento para crear cuentas de endpoint.



Haga clic en " Agregar una función de aprovisionamiento '- > Buscar por el papel y presentar

Vaya a Inicio-> Ver Mis tareas Enviado para verificar si se completa con éxito la tarea



Included Events

	Event Name	Description	Status	Submitted	Last Updated	Last Activity
	Create user	Create user "tst126prd3"	Completed	12/14/2012 6:37 PM	12/14/2012 6:37 PM	
	Assign user admin role	Assign user "tst126prd3" admin role "IADB AUDITOR"	Completed	12/14/2012 6:37 PM	12/14/2012 6:37 PM	
	Assign user provisioning role	Assign user "tst126prd3" provisioning role "HURISStdUser_TSTDBMS1"	Completed	12/14/2012 6:37 PM	12/14/2012 6:37 PM	Global User 'tst126prd3' modified successfully
	Assign user provisioning role	Assign user "tst126prd3" provisioning role "HURISUser_ORA_PSPROD"	Completed	12/14/2012 6:37 PM	12/14/2012 6:37 PM	Global User 'tst126prd3' modified successfully
	Assign user provisioning role	Assign user "tst126prd3" provisioning role "ITEIDBPrepUserNoMail"	Completed	12/14/2012 6:37 PM	12/14/2012 6:37 PM	Global User 'tst126prd3' modified successfully
	Synchronize user	Synchronize user "tst126prd3"	Completed	12/14/2012 6:37 PM	12/14/2012 6:37 PM	
	Synchronize user attributes with accounts	Synchronize user "tst126prd3" attributes with accounts	Completed	12/14/2012 6:37 PM	12/14/2012 6:37 PM	Global User 'tst126prd3' and associated account statuses updated successfully: (accounts updated: 0, failures: 0)

Identity Policy Violations

Identity Policy Name	Type	Workflow Status	Message
No results.			

Un correo electrónico será enviado a las personas competentes que la creación de usuarios con éxito

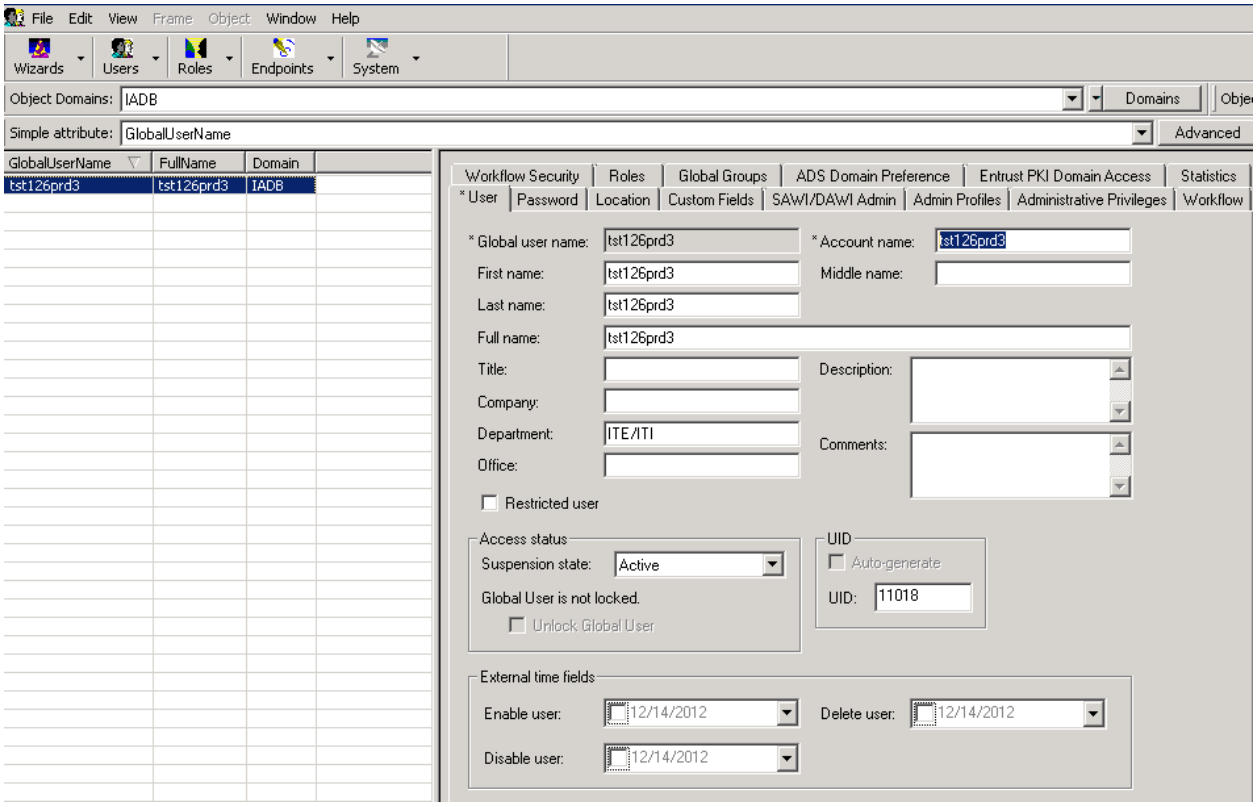
From: eTrust Admin
Sent: Friday, December 14, 2012 6:37 PM
To: ITE Client Center (ICC); Information Security; EMail Group
Subject: New AD Account tst126prd3 Created

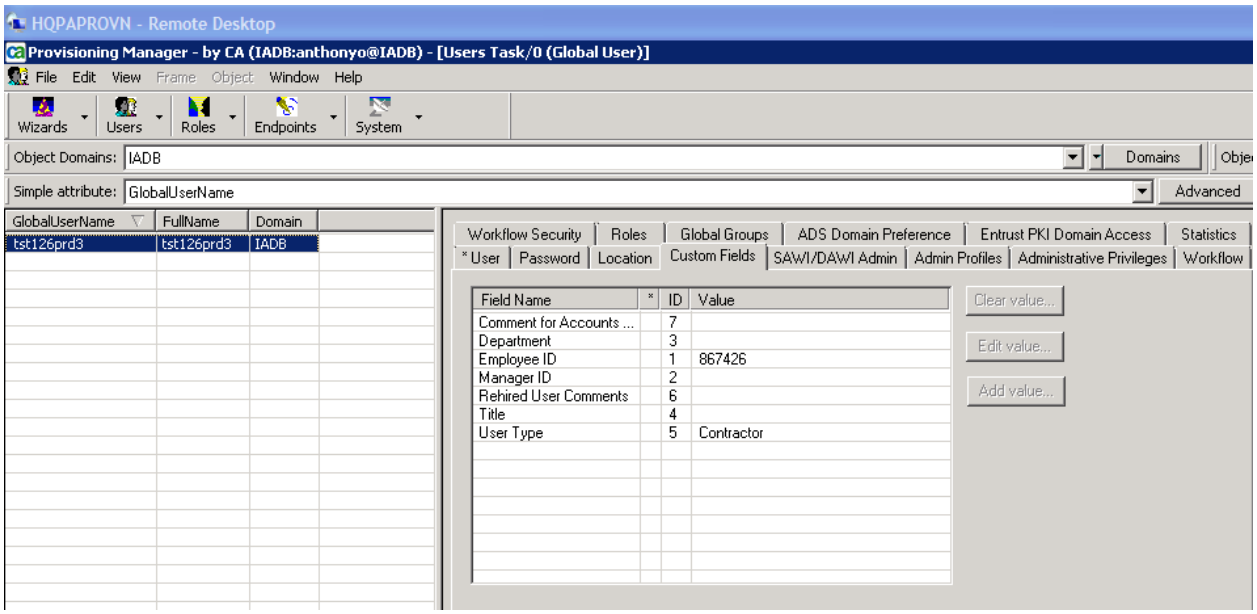
Automatic email from Identity Manager.
****

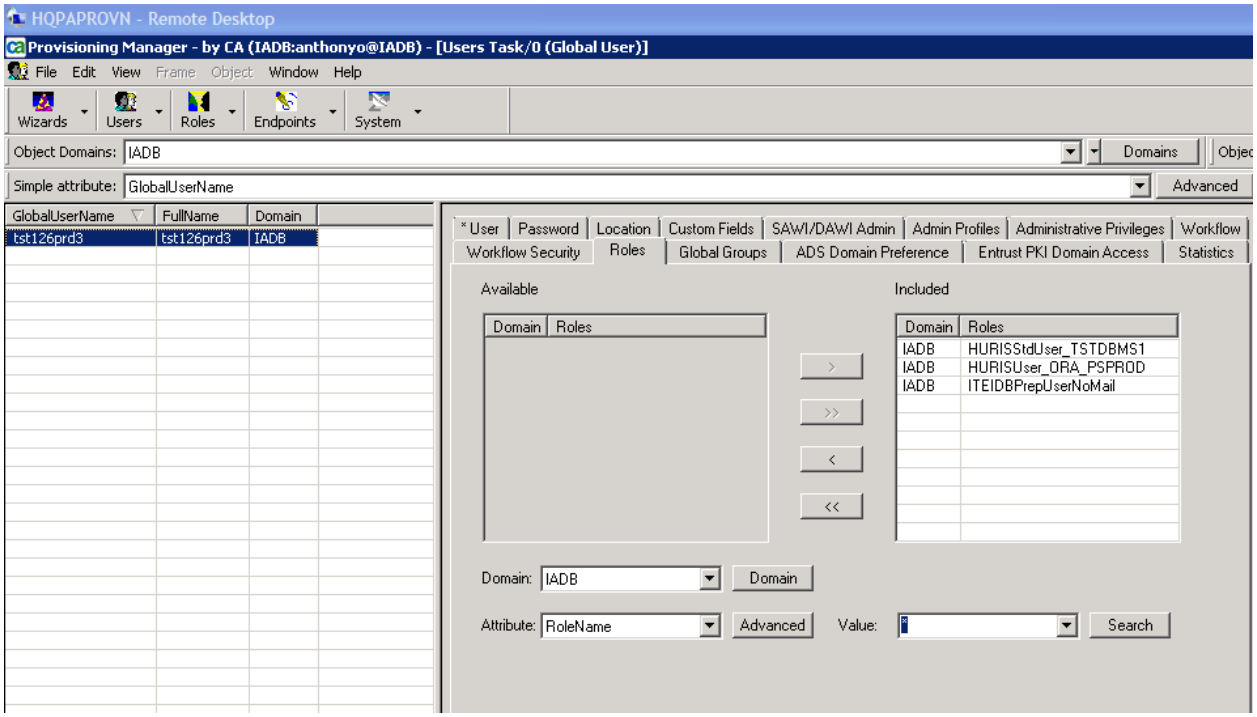
Create New User

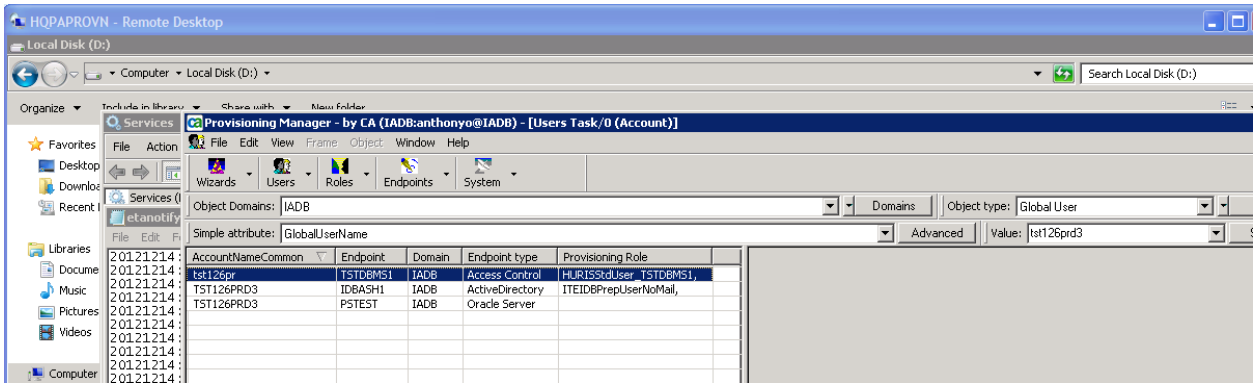
User ID = **tst126prd3**
Full Name = **tst126prd3**
Employee ID = **867426**
Org Unit = **ITE/ITI**
User Type = **Contractor**

Otras validaciones en Provisioning Manager / Endpoints


File Edit View Frame Object Window Help
Wizards
Users
Roles
Endpoints
System
Object Domains: IADB
Domains
Simple attribute: GlobalUserName
Advanced
GlobalUserName
FullName
Domain
tst126prd3
tst126prd3
IADB
Workflow Security
Roles
Global Groups
ADS Domain Preference
Entrust PKI Domain Access
Statistics
* User
Password
Location
Custom Fields
SAWI/DAWI Admin
Admin Profiles
Administrative Privileges
Workflow
* Global user name:
tst126prd3
* Account name:
tst126prd3
First name:
tst126prd3
Middle name:
Last name:
tst126prd3
Full name:
tst126prd3
Title:
Description:
Company:
Department:
ITE/ITI
Comments:
Office:
Restricted user
Access status
Suspension state:
Active
Global User is not locked.
Unlock Global User
UID
Auto-generate
UID:
11018
External time fields
Enable user:
12/14/2012
Delete user:
12/14/2012
Disable user:
12/14/2012


HQPAPROVN - Remote Desktop
Provisioning Manager - by CA (IADB:anthonyo@IADB) - [Users Task/0 (Global User)]
File Edit View Frame Object Window Help
Wizards
Users
Roles
Endpoints
System
Object Domains: IADB
Domains
Simple attribute: GlobalUserName
Advanced
GlobalUserName
FullName
Domain
tst126prd3
tst126prd3
IADB
Workflow Security
Roles
Global Groups
ADS Domain Preference
Entrust PKI Domain Access
Statistics
* User
Password
Location
Custom Fields
SAWI/DAWI Admin
Admin Profiles
Administrative Privileges
Workflow
Field Name
*
ID
Value
Comment for Accounts ...
7
Department
3
Employee ID
1
867426
Manager ID
2
Rehired User Comments
6
Title
4
User Type
5
Contractor
Clear value...
Edit value...
Add value...

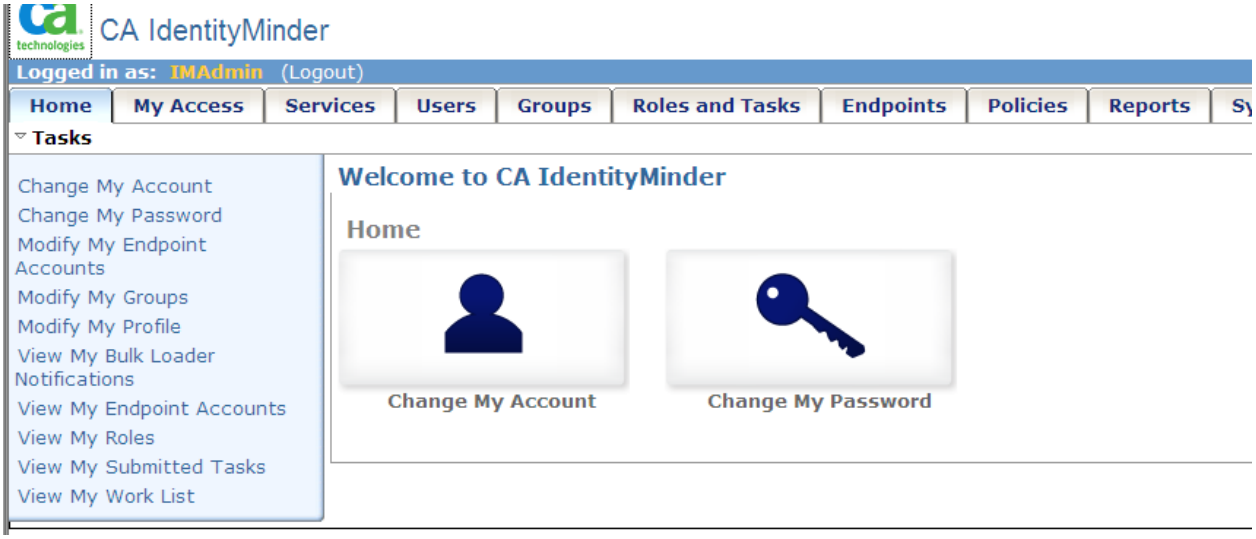




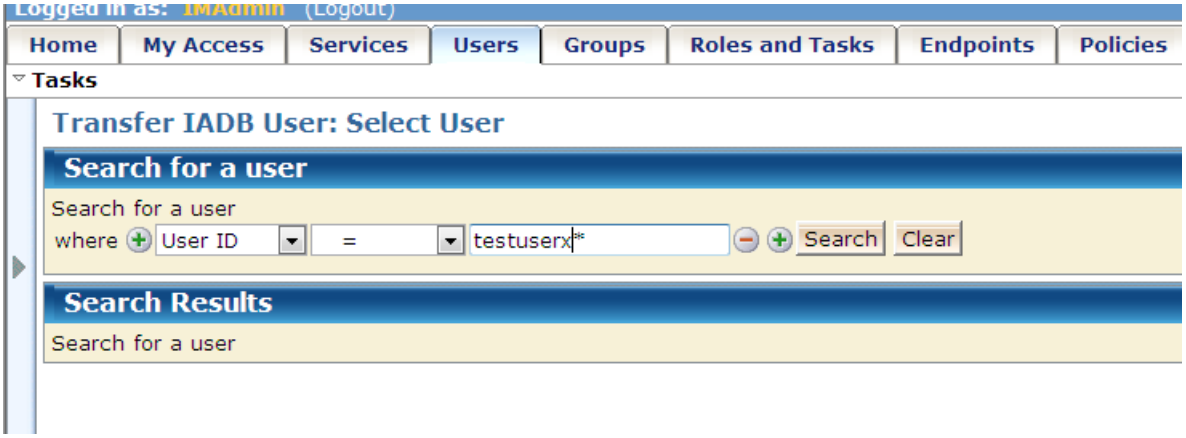
17.2 Transferencia BID de usuario

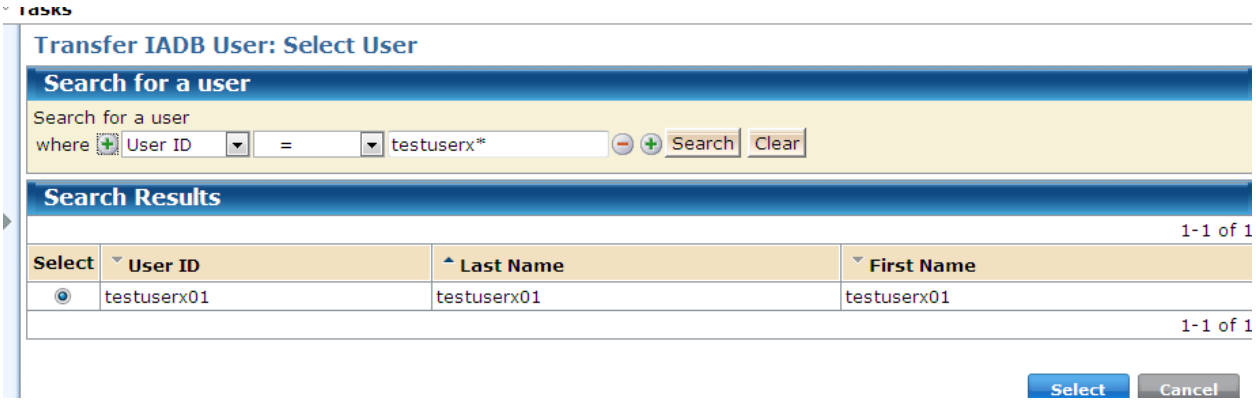
Utilice esta tarea cuando un usuario cambia de un departamento a otro .

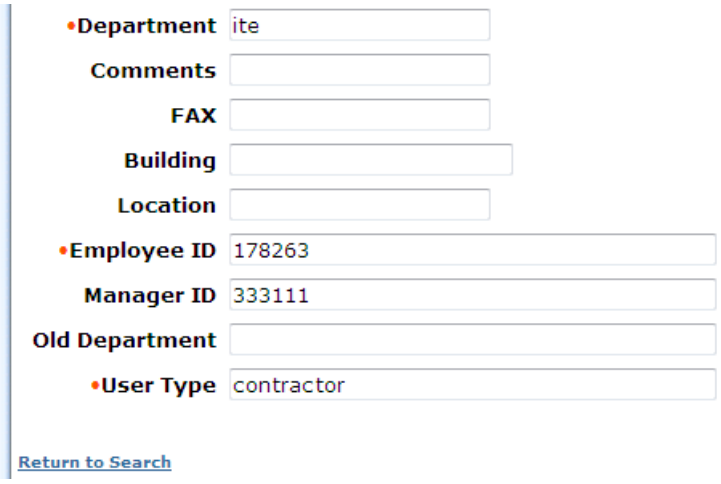
Inicia sesión para la consola de usuario de Identity Manager como un usuario administrador



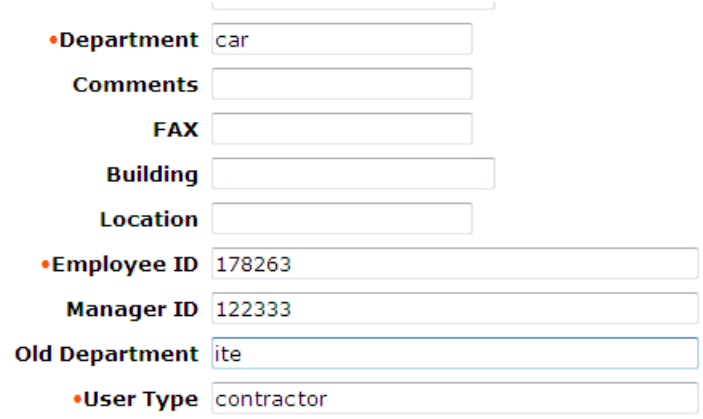
Busque Usuarios- > Administrar usuarios- > Traslado BID usuario







Actualizar el formulario de transferencia y pulse enviar



Presentar la solicitud.

Compruebe que se ha completado con éxito la tarea. Vaya a Inicio-> ver Tareas enviadas > Buscar

Identity Manager enviará un correo electrónico a las personas pertinentes al término

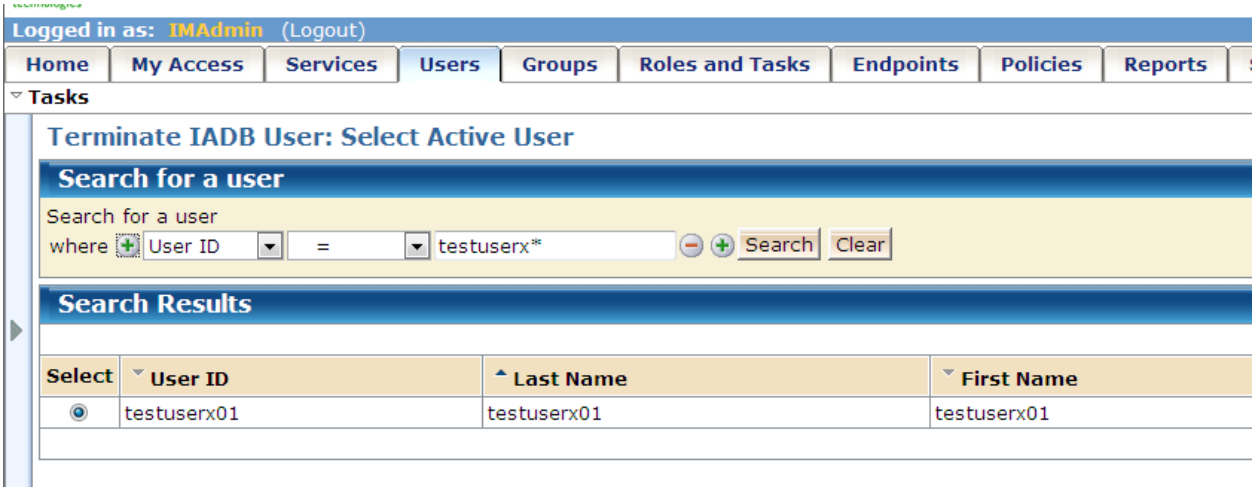
17.3 Terminación de Usuarios

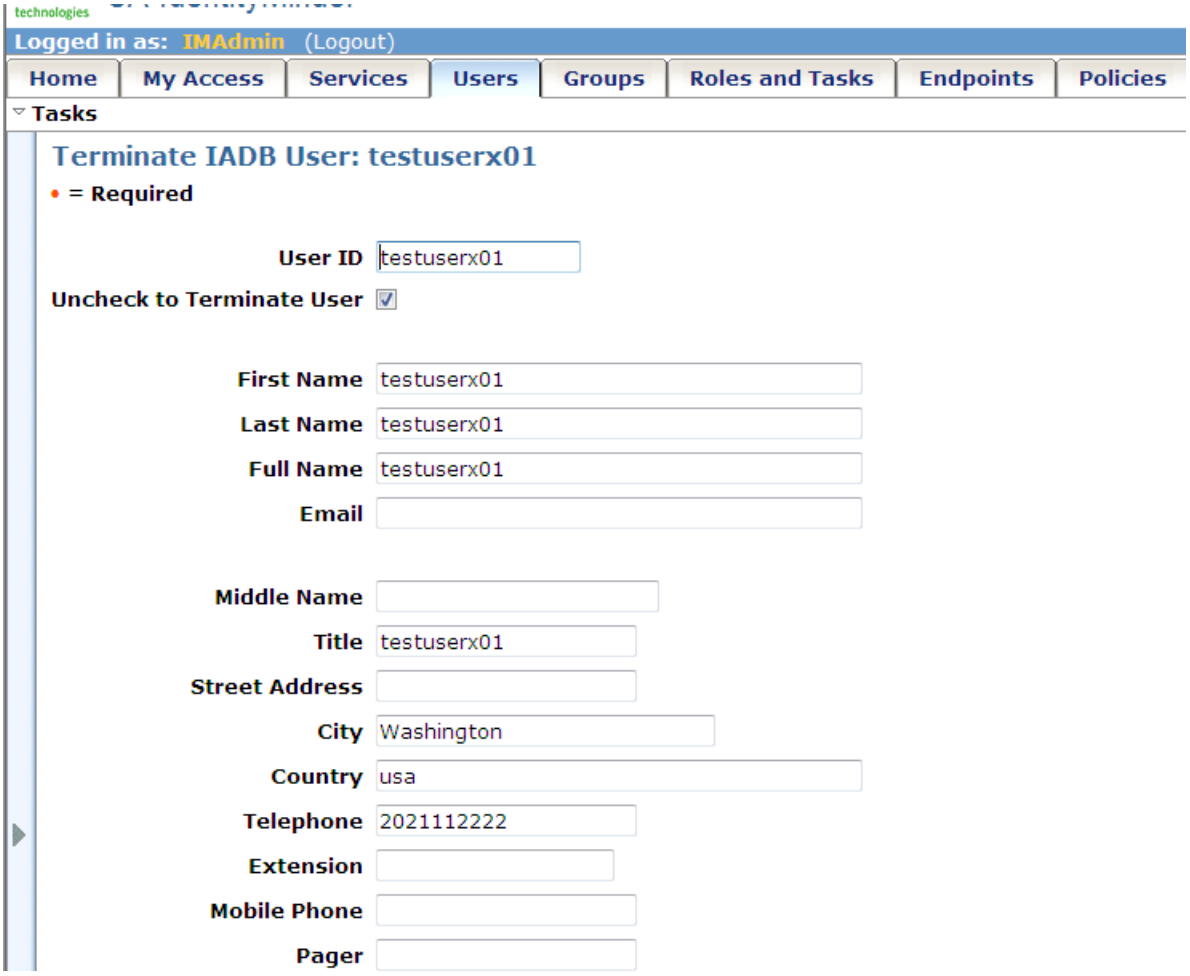
Utilice esta tarea para poner fin a un usuario. Tenga en cuenta que esta tarea no elimina los usuarios en los puntos finales (si el usuario se ha asignado anteriormente aprovisionamiento papeles) , pero sólo se desactivará los usuarios.

Inicia sesión para consola de usuario de Identity Manager como administrador.

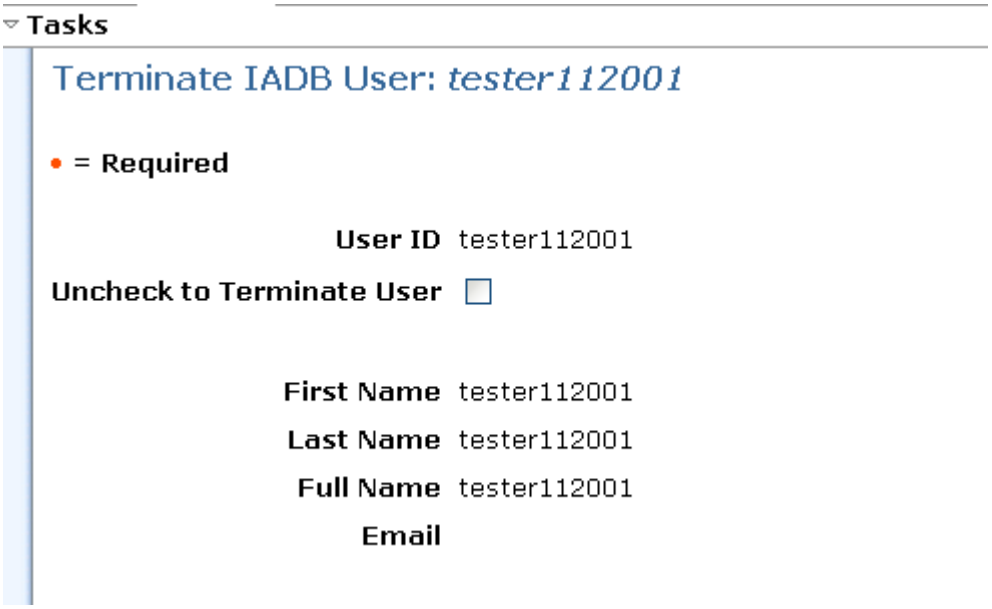
Busque Usuarios- > Administrar usuarios- > Terminar BID usuario

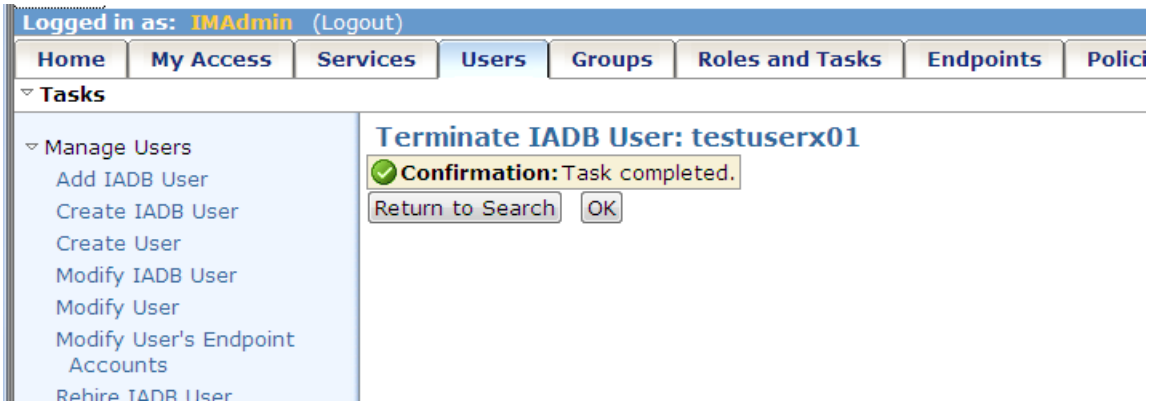
Buscar en el usuario para terminar





Desactive la casilla de verificación en el formulario y pulse enviar





Después de completar con éxito , Identity Manager envía un correo electrónico a los usuarios respectivos / administradores .

17.4 Recontratación de usuario

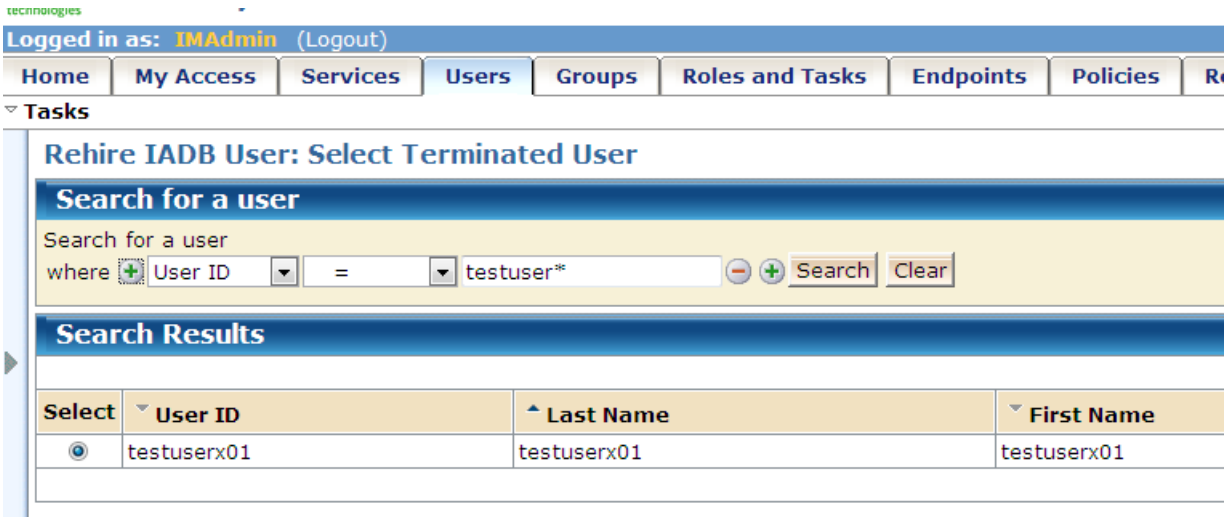
Utilice esta tarea para volver a contratar a un usuario , que se dio por terminado con anterioridad.

Inicia sesión para consola de usuario de Identity Manager como administrador

Busque Usuarios- > Administrar usuarios- > recontratación BID Usuario-> Busca el usuario

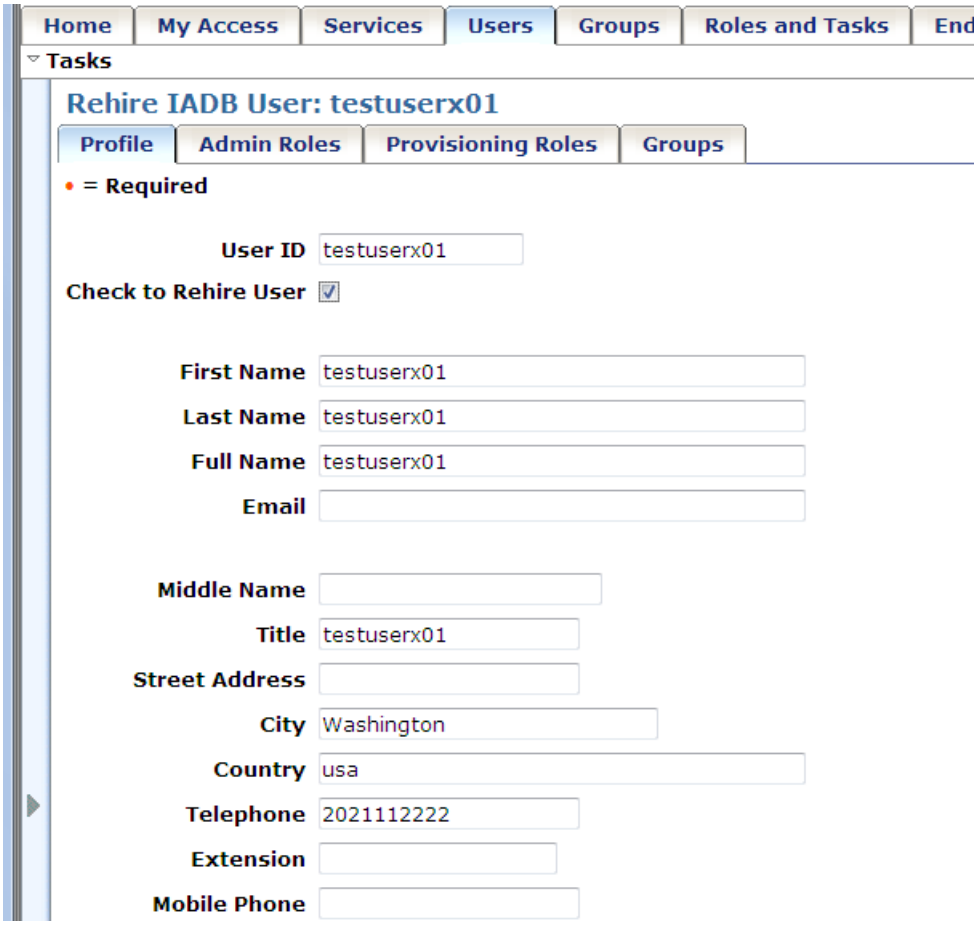
Nota: La búsqueda sería sólo los usuarios de visualización que fueron despedidos con anterioridad

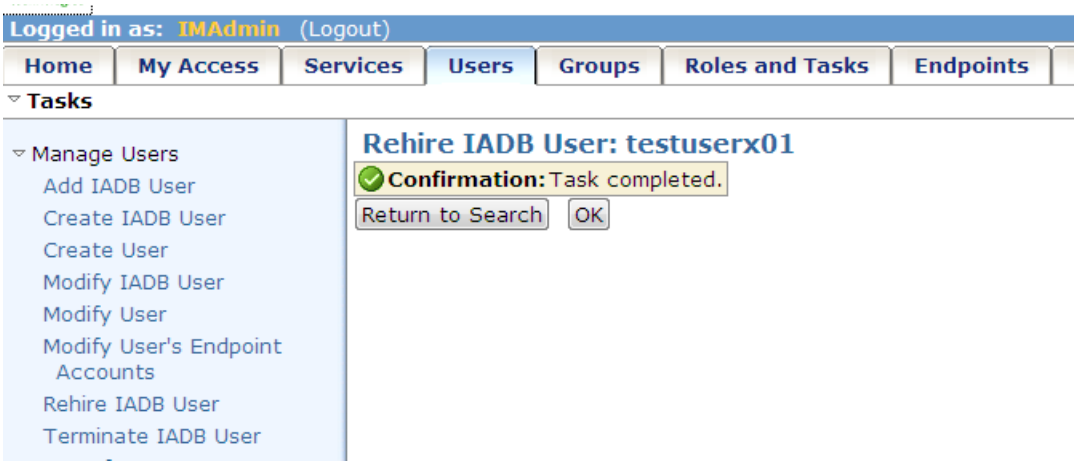
Esta tarea de recrear el TDA / Buzón , si falta, por aprovisionamiento de asignación de funciones . El rol de aprovisionamiento sólo puede ser añadido después de la tarea de usuario recontratación BID completado con éxito .



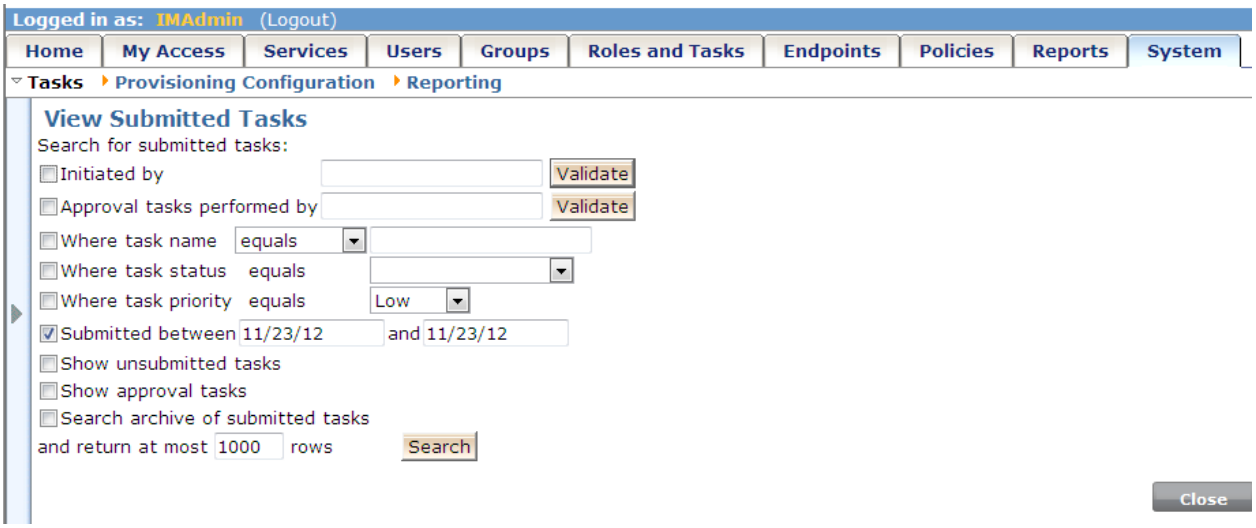
Seleccione la casilla de verificación y pulse enviar volver a contratar el usuario

171


Home
My Access
Services
Users
Groups
Roles and Tasks
End
Tasks
Rehire IADB User: testuserx01
Profile
Admin Roles
Provisioning Roles
Groups
• = Required
User ID testuserx01
Check to Rehire User
First Name testuserx01
Last Name testuserx01
Full Name testuserx01
Email
Middle Name
Title testuserx01
Street Address
City Washington
Country usa
Telephone 2021112222
Extension
Mobile Phone


Logged in as: IMAdmin (Logout)
Home
My Access
Services
Users
Groups
Roles and Tasks
Endpoints
Tasks
Manage Users
Add IADB User
Create IADB User
Create User
Modify IADB User
Modify User
Modify User's Endpoint Accounts
Rehire IADB User
Terminate IADB User
Rehire IADB User: testuserx01
Confirmation: Task completed.
Return to Search
OK

Enviando tareas



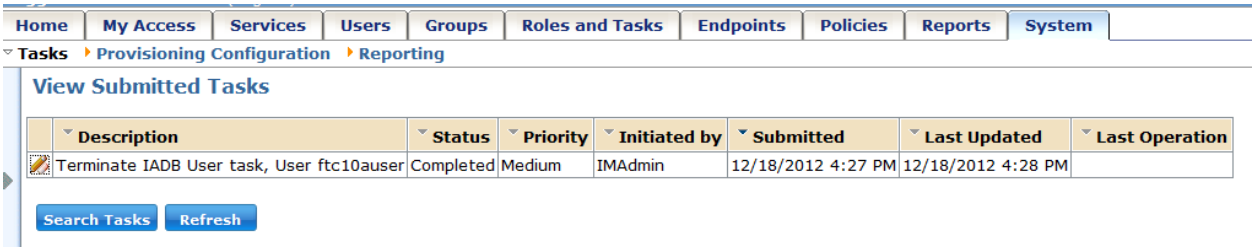
Despus de completar con éxito , Identity Manager envía una notificación por correo electrónico a los respectivos usuarios / administradores.

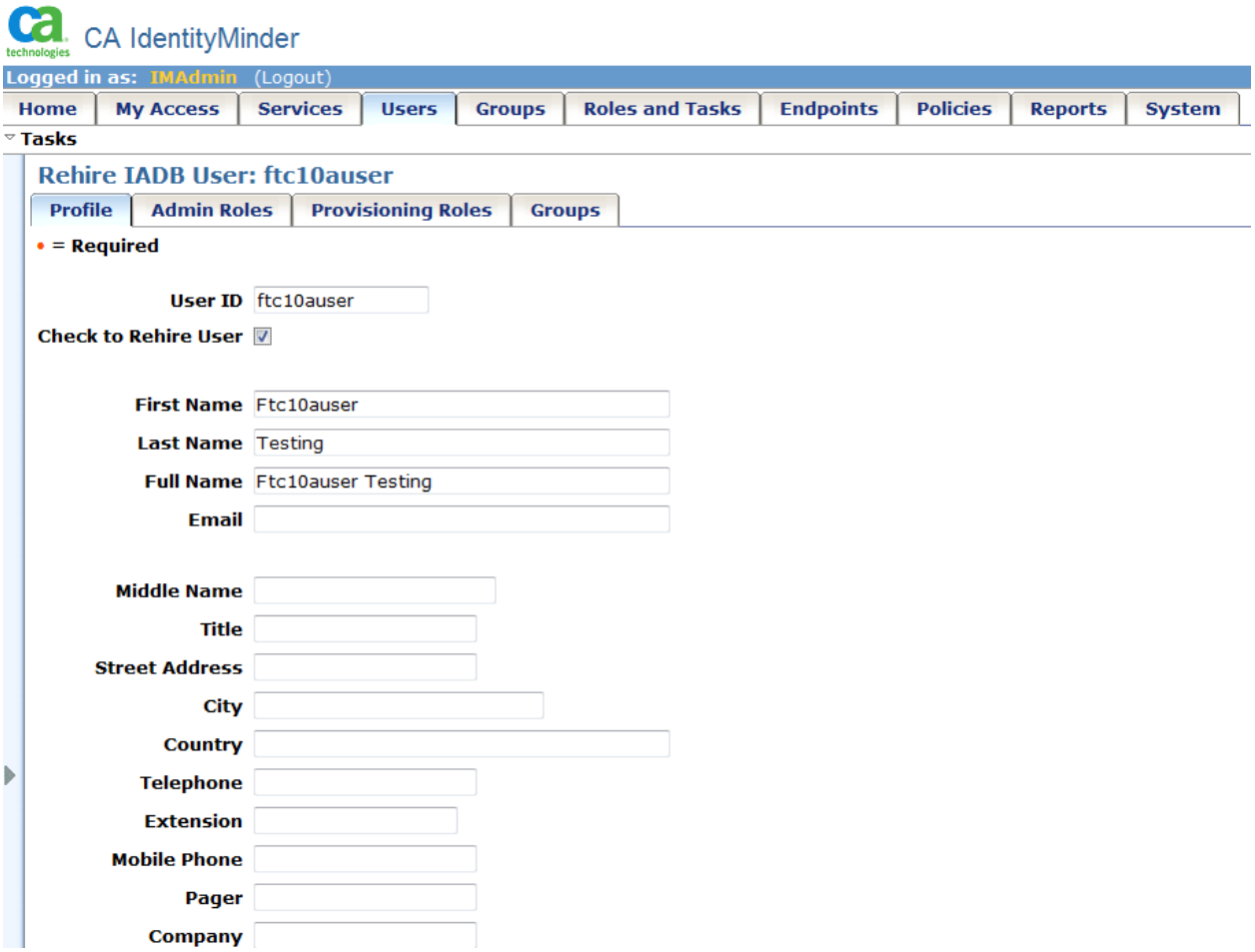
17.4.1 Roles recontratación y Actualización de aprovisionamiento

Recontratación y actualización de funciones de aprovisionamiento se puede realizar en un solo paso ahora a diferencia de la versión anterior del IDM en el que el primer paso era volver a contratar

el usuario y en el segundo paso , actualizar las funciones de aprovisionamiento . Tratar de hacer esto dio lugar a error a continuación

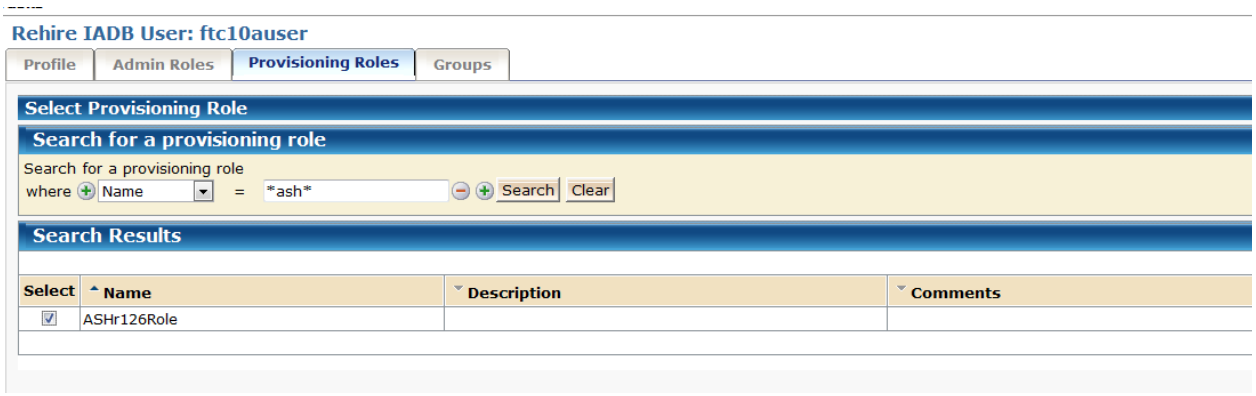
Se realizó una prueba en IDM r12.6

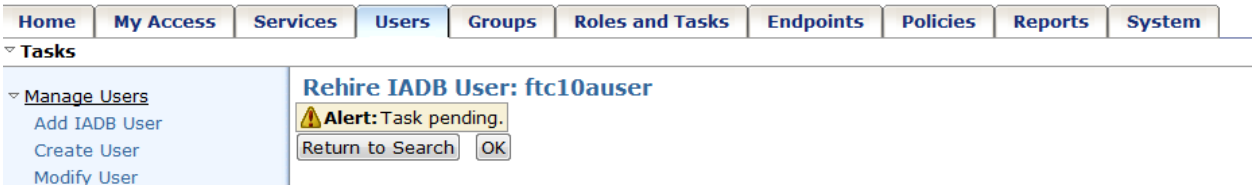




Antes del cmabio,

Después de asignar roles de aprovisionamiento.





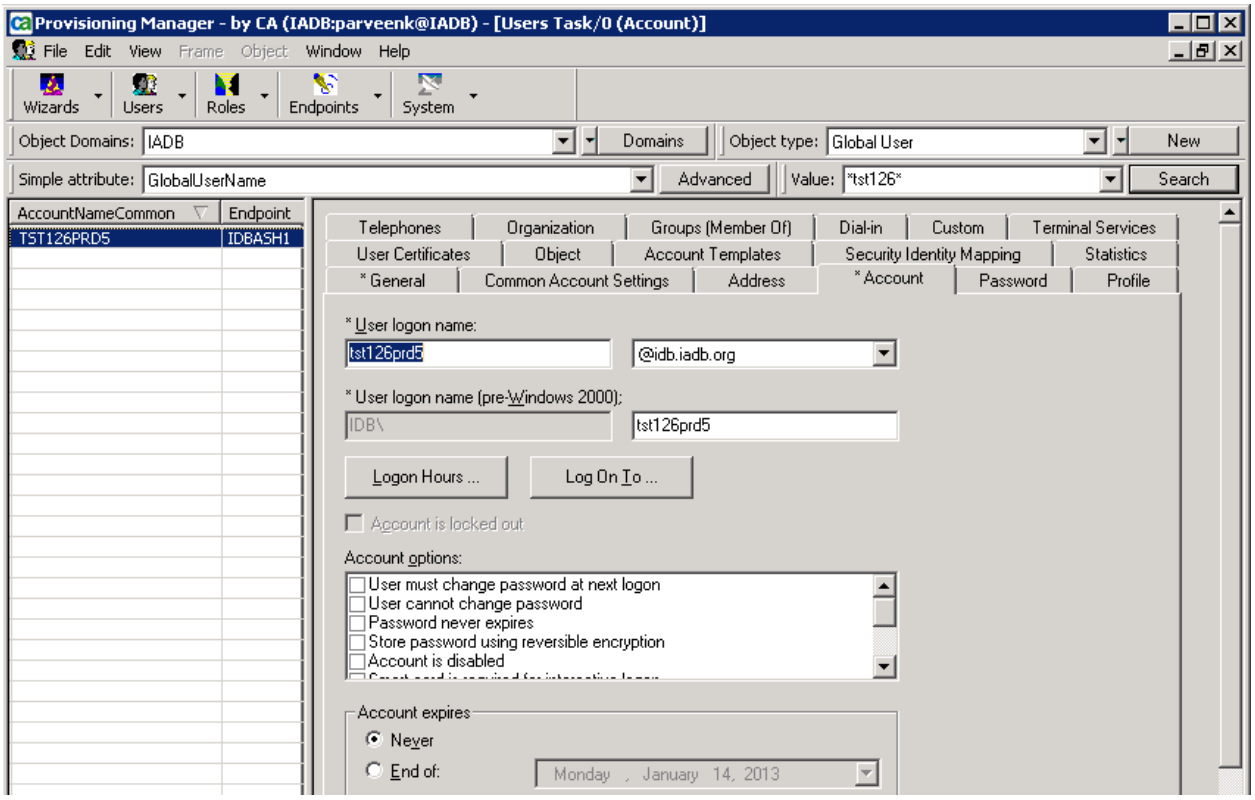
La cuenta se a creado correctamente como se ve en las siguientes imagenes.

176

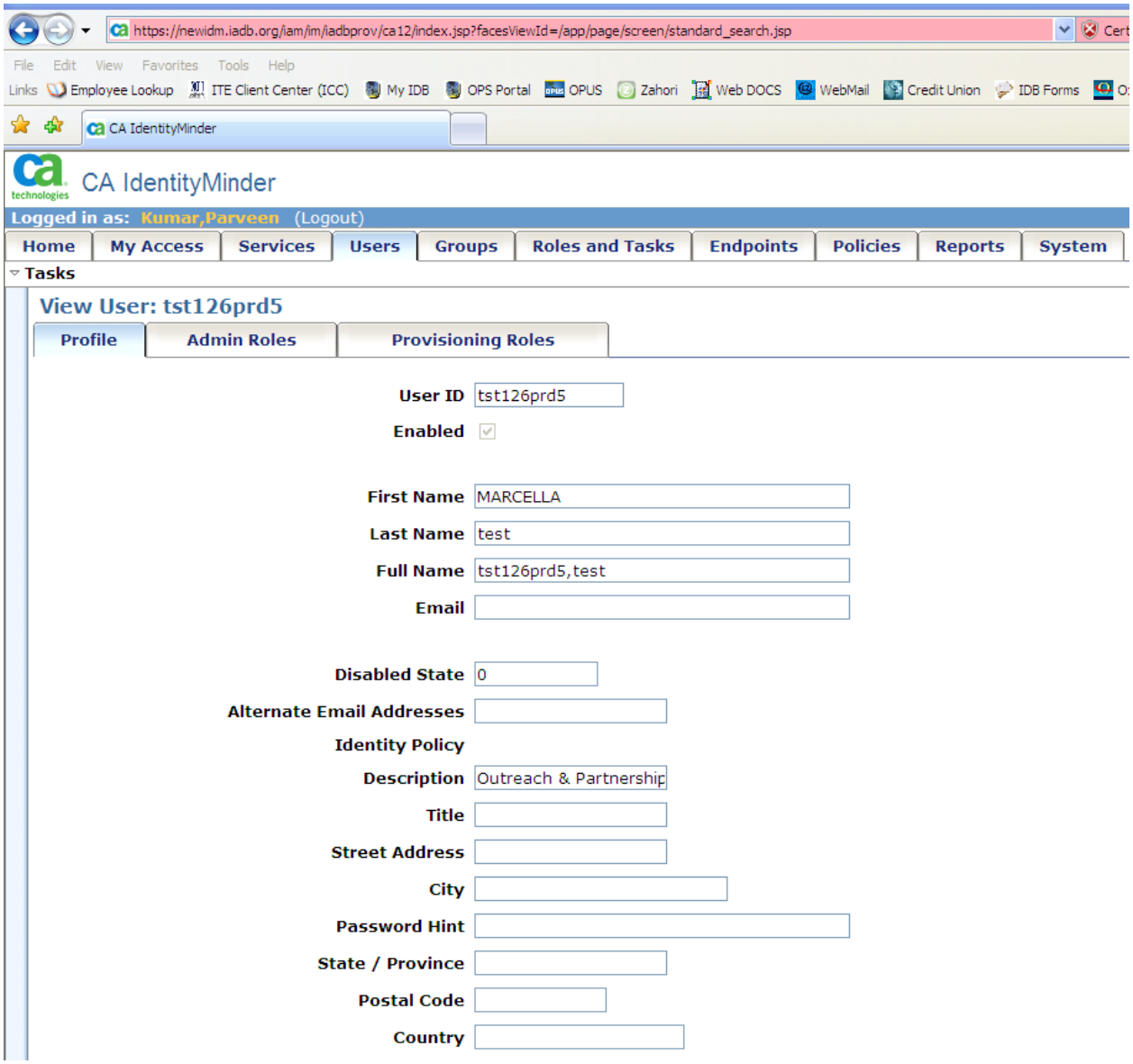
18 Interface de PSFEED

18.1 Agregar usuario de provisionamiento IADB

Esta tarea de administración se activa mediante la creación de un nuevo usuario para integrarse con los procesos PSFEED lotes ejecutados desde la máquina del servidor de aprovisionamiento. El objetivo de esta tarea es crear el usuario en el Minder Directorio de Identidad Corporativa mediante comandos ETAUTIL . Esta tarea también está configurado para las notificaciones de correo electrónico .



177



18.2 Modificación de un usuario de IADB provisionado en PSFEED

Esta tarea se disparada cuando corre cualquiera de los procesos tal como: Transferencias, terminaciones, recontrataciones, actualizaciones via el PSFEED corriendo el lote de archivos de el provisioning server.

ControlSTAFFpartial.bat

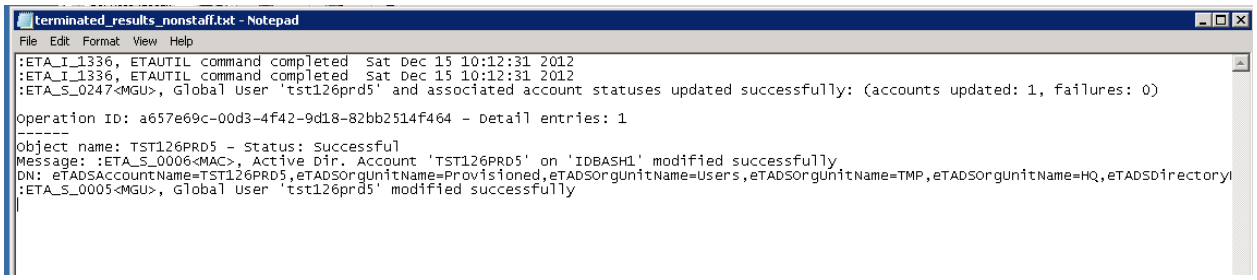
ControlNonStaffpartial.bat

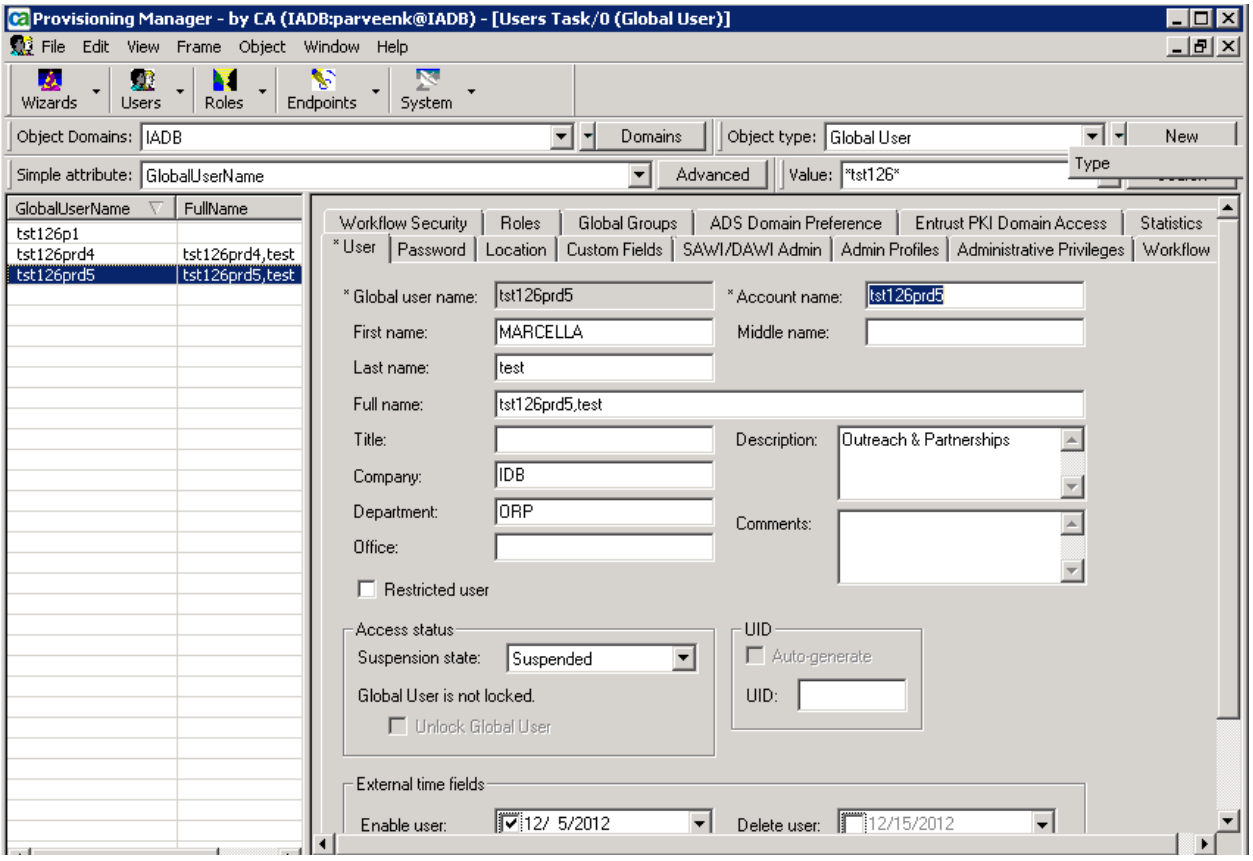
178

El proposito de está tarea es realizar transferencias/terminaciones/recontrataciones de usuarios que son requeridos desde la fuente del provisionig people soft, la tarea se corre en el servidor de provisionamiento an también está configurada para que envie notificaciones de email.

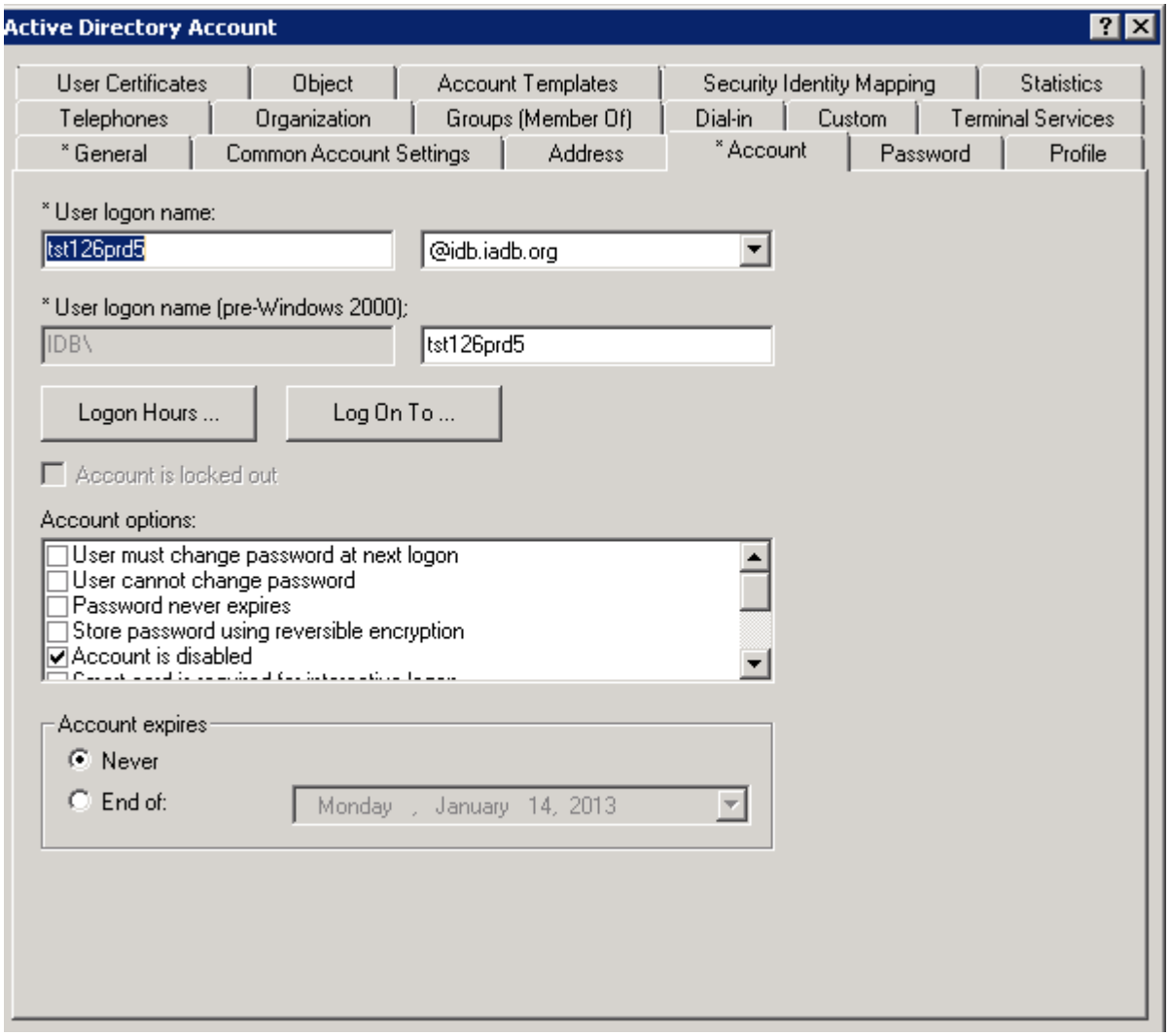
18.2.1 Terminar usuarios

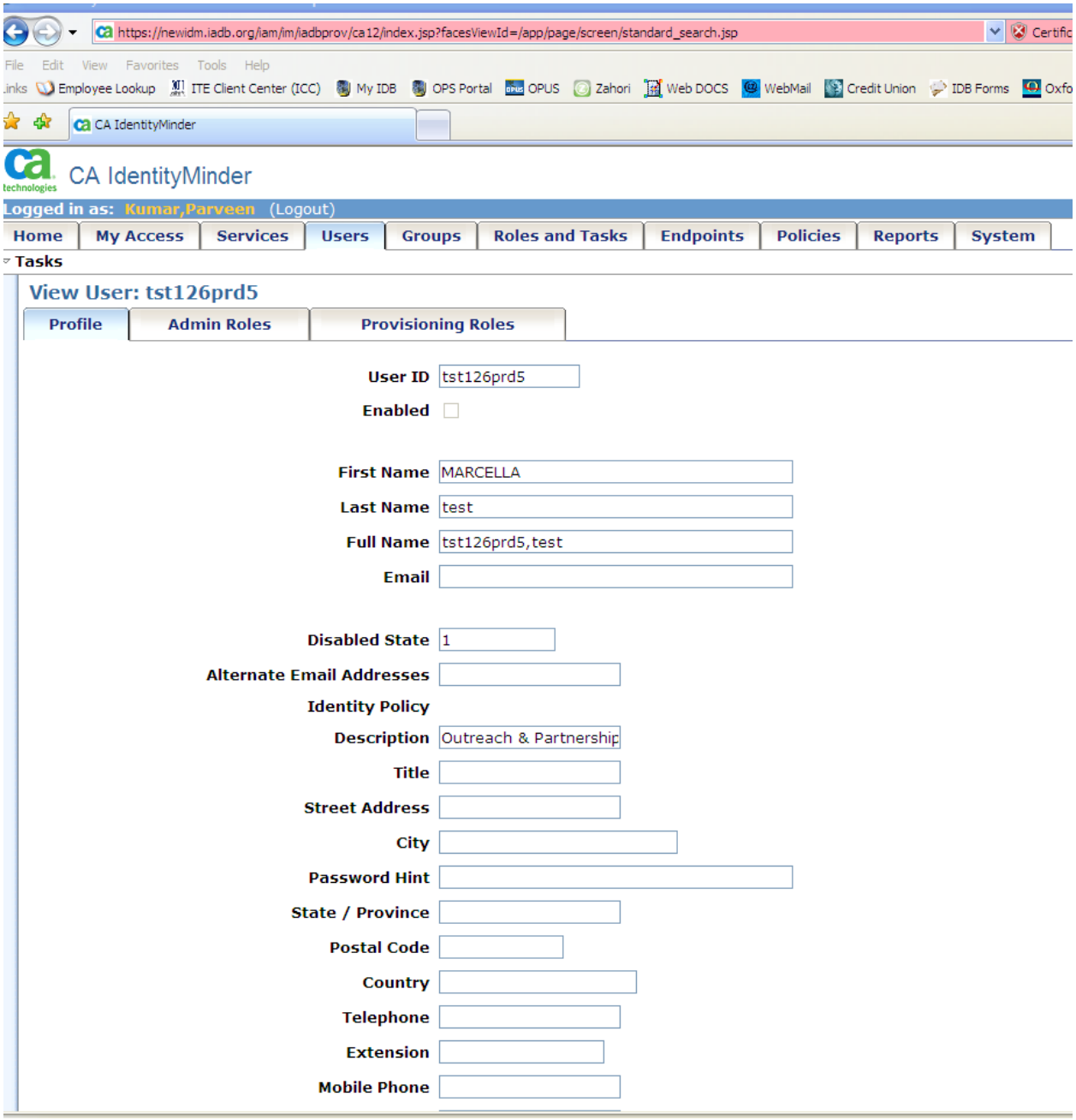
Archivo de alimentación separada para terminar ususarios en procesador por PSFeed con codigos personalizados, siga los pasos siguientes de verificación.

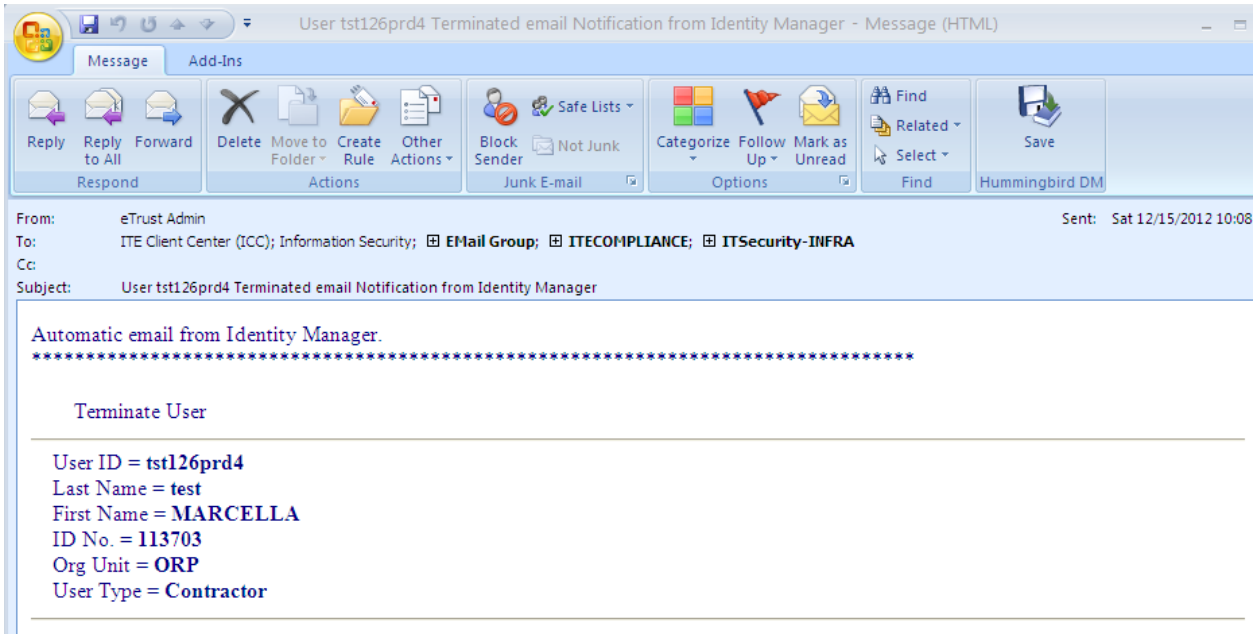




179

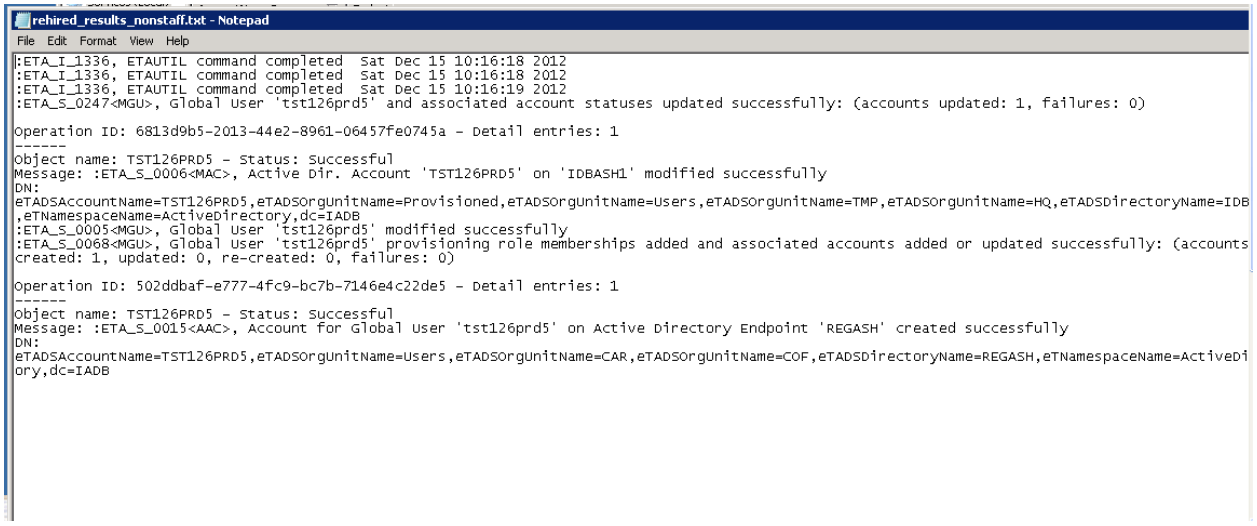

Active Directory Account
User Certificates
Object
Account Templates
Security Identity Mapping
Statistics
Telephones
Organization
Groups (Member Of)
Dial-in
Custom
Terminal Services
* General
Common Account Settings
Address
* Account
Password
Profile
* User logon name:
tst126prd5
@idb.iadb.org
* User logon name (pre-Windows 2000):
IDB\
tst126prd5
Logon Hours ...
Log On To ...
Account is locked out
Account options:
User must change password at next logon
User cannot change password
Password never expires
Store password using reversible encryption
Account is disabled
Account expires
Never
End of:
Monday , January 14, 2013

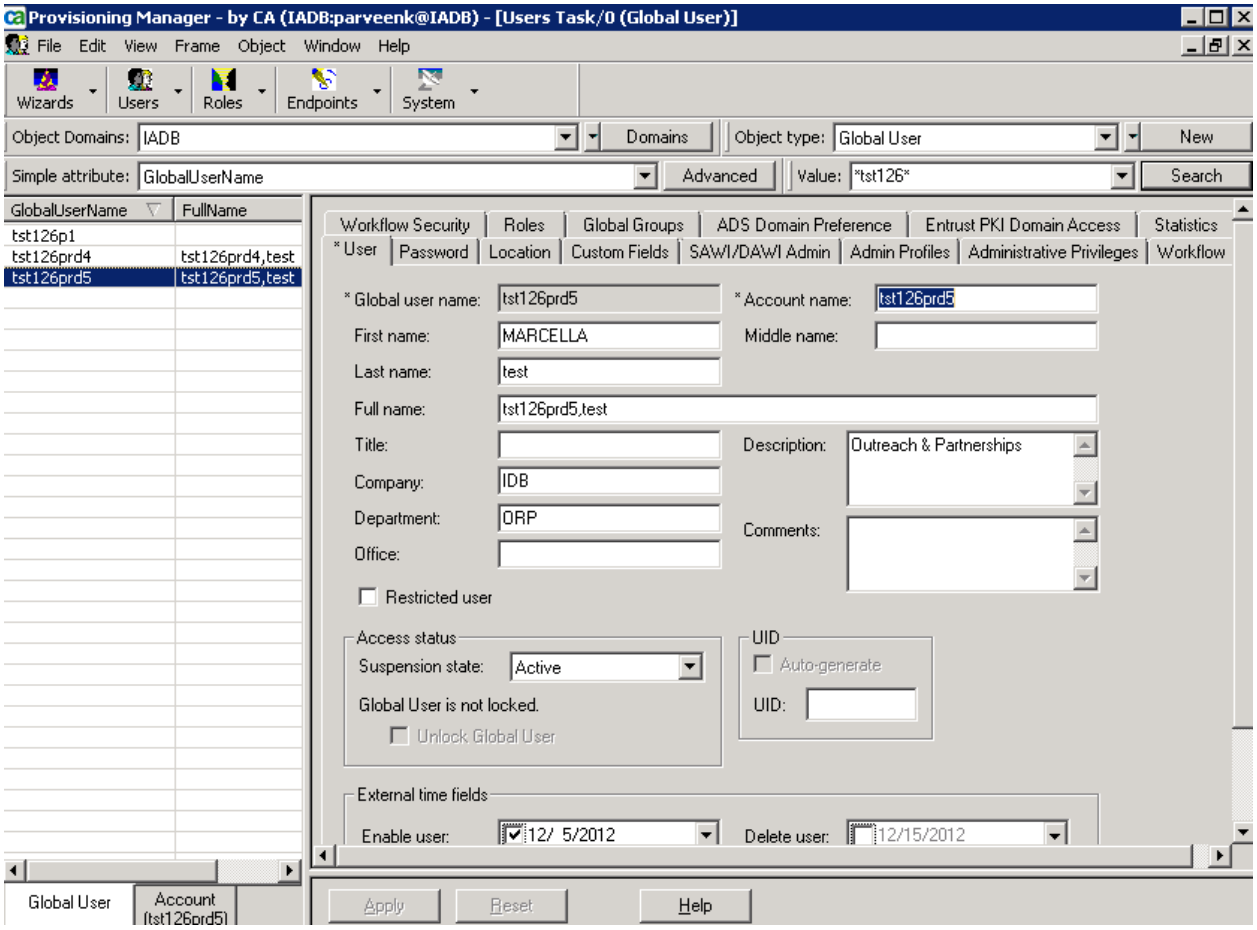

https://newidm.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/screen/standard_search.jsp
File Edit View Favorites Tools Help
Employee Lookup
ITE Client Center (ICC)
My IDB
OPS Portal
OPUS
Zahori
Web DOCS
WebMail
Credit Union
IDB Forms
CA IdentityMinder
CA IdentityMinder
Logged in as: Kumar,Parveen (Logout)
Home
My Access
Services
Users
Groups
Roles and Tasks
Endpoints
Policies
Reports
System
Tasks
View User: tst126prd5
Profile
Admin Roles
Provisioning Roles
User ID tst126prd5
Enabled
First Name MARCELLA
Last Name test
Full Name tst126prd5,test
Email
Disabled State 1
Alternate Email Addresses
Identity Policy
Description Outreach & Partnership
Title
Street Address
City
Password Hint
State / Province
Postal Code
Country
Telephone
Extension
Mobile Phone

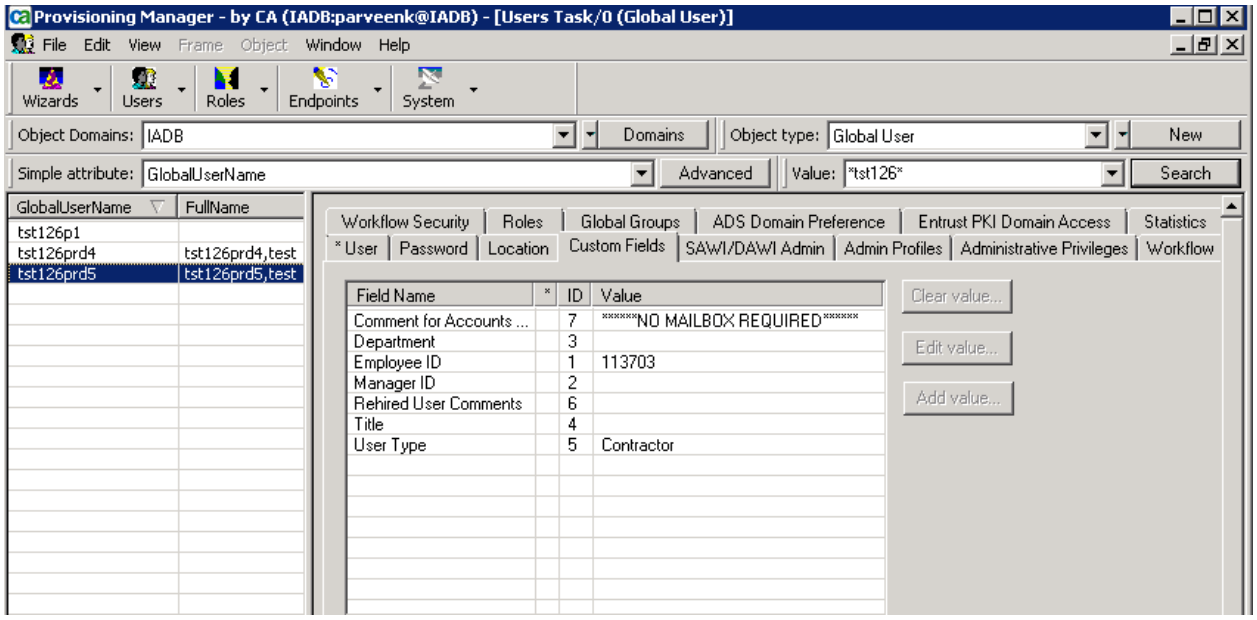


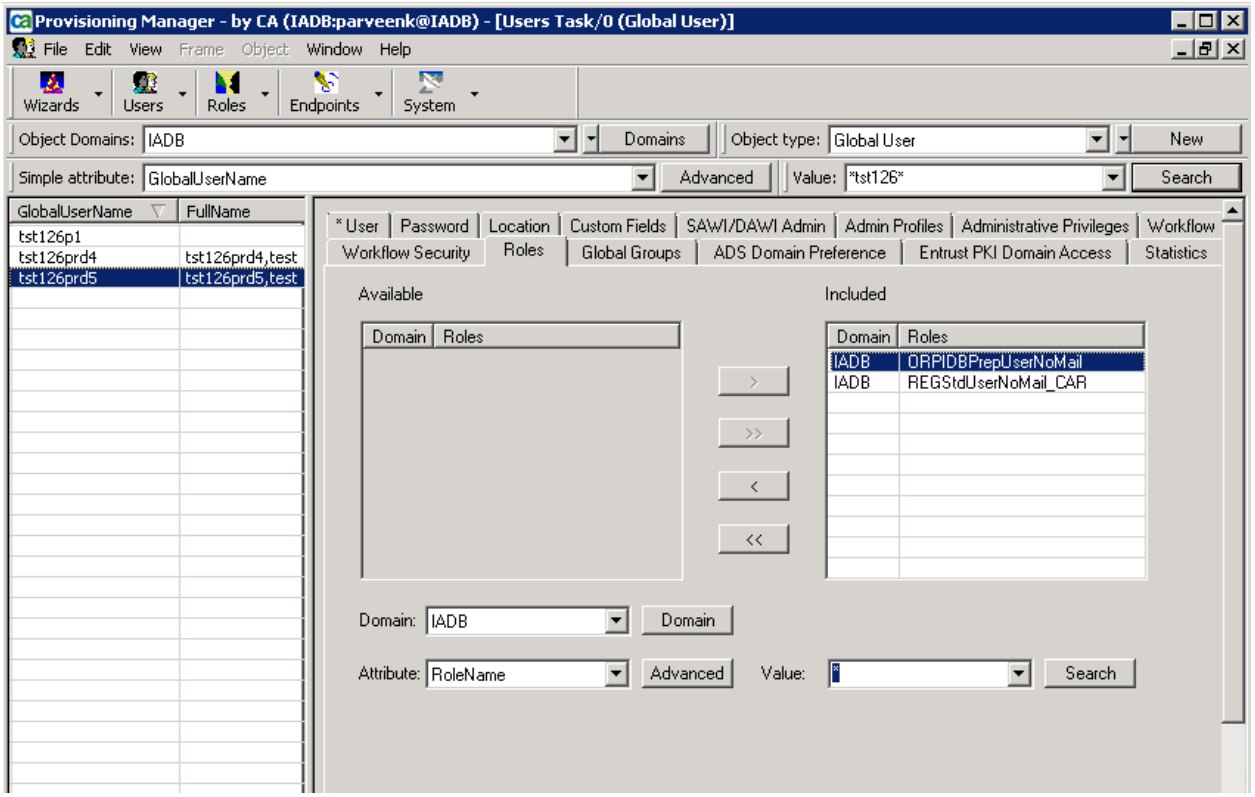
18.2.2 Reinstalar usuario

Seguir el proceso para la reinstalación del usuario



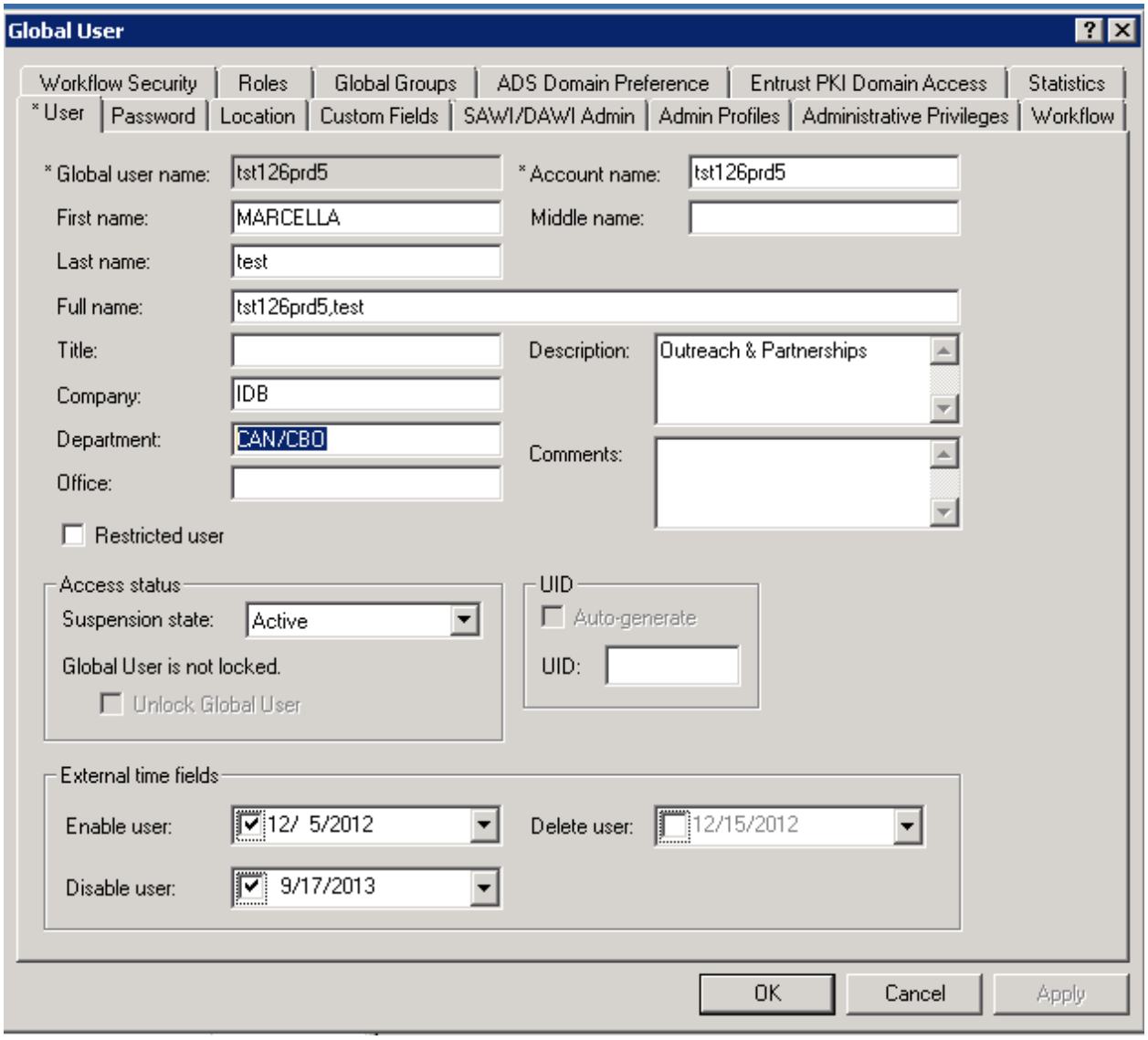

Provisioning Manager - by CA (IADB:parveenk@IADB) - [Users Task/0 (Global User)]
File Edit View Frame Object Window Help
Wizards Users Roles Endpoints System
Object Domains: IADB Domains Object type: Global User New
Simple attribute: GlobalUserName Advanced Value: *tst126* Search
GlobalUserName FullName
tst126p1
tst126prd4 tst126prd4,test
tst126prd5 tst126prd5,test
Workflow Security Roles Global Groups ADS Domain Preference Entrust PKI Domain Access Statistics
* User Password Location Custom Fields SAWI/DAWI Admin Admin Profiles Administrative Privileges Workflow
* Global user name: tst126prd5
* Account name: tst126prd5
First name: MARCELLA
Middle name:
Last name: test
Full name: tst126prd5,test
Title:
Description: Outreach & Partnerships
Company: IDB
Department: ORP
Comments:
Office:
Restricted user
Access status
Suspension state: Active
Global User is not locked.
Unlock Global User
UID
Auto-generate
UID:
External time fields
Enable user: 12/ 5/2012
Delete user: 12/15/2012
Global User
Account (tst126prd5)
Apply Reset Help

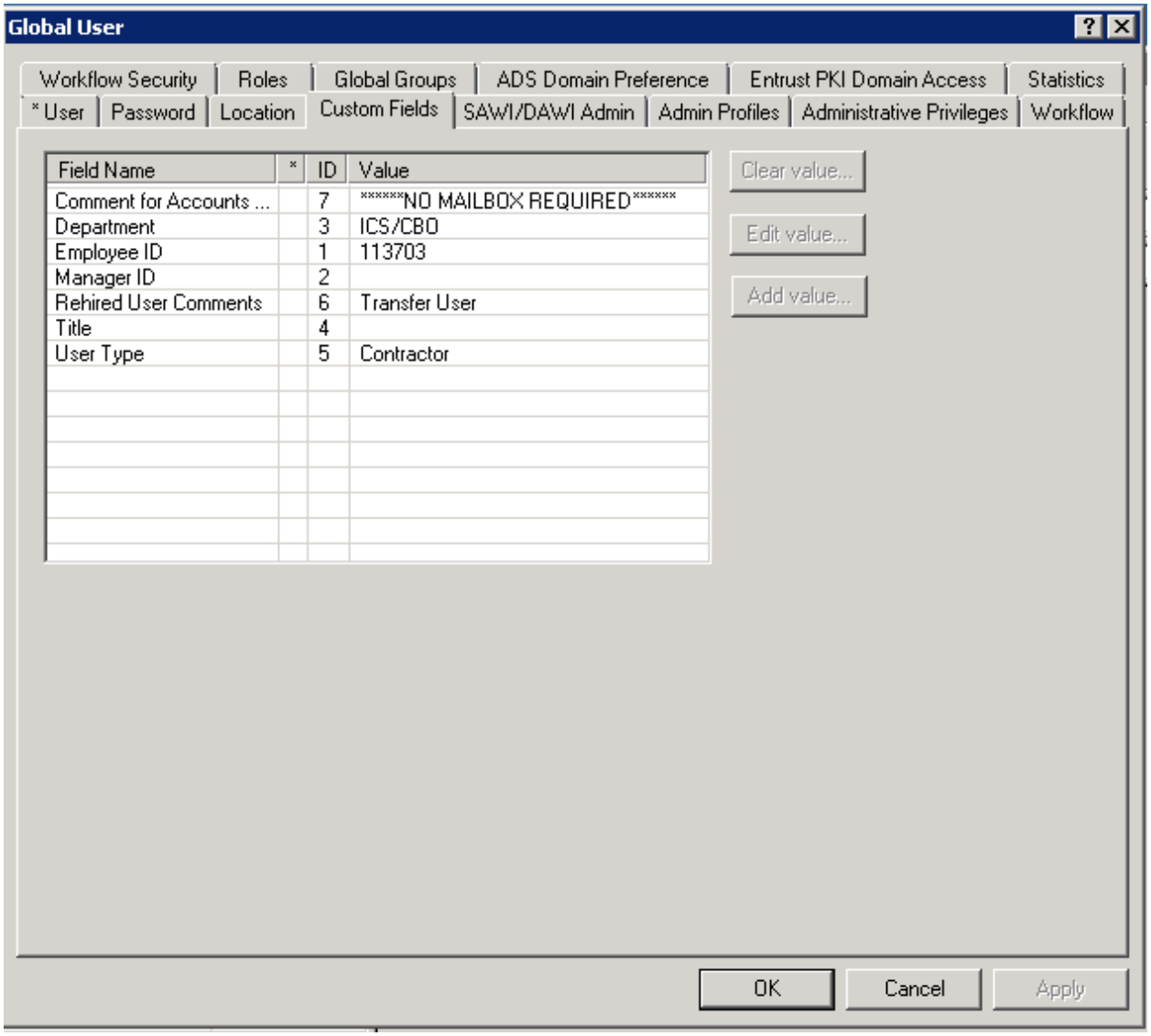

Provisioning Manager - by CA (IADB:parveenk@IADB) - [Users Task/0 (Global User)]
File Edit View Frame Object Window Help
Wizards Users Roles Endpoints System
Object Domains: IADB Domains Object type: Global User New
Simple attribute: GlobalUserName Advanced Value: *tst126* Search
GlobalUserName FullName
tst126p1
tst126prd4 tst126prd4,test
tst126prd5 tst126prd5,test
Workflow Security Roles Global Groups ADS Domain Preference Entrust PKI Domain Access Statistics
* User Password Location Custom Fields SAWI/DAWI Admin Admin Profiles Administrative Privileges Workflow
Field Name * ID Value
Comment for Accounts ... 7 ******NO MAILBOX REQUIRED******
Department 3
Employee ID 1 113703
Manager ID 2
Rehired User Comments 6
Title 4
User Type 5 Contractor
Clear value...
Edit value...
Add value...

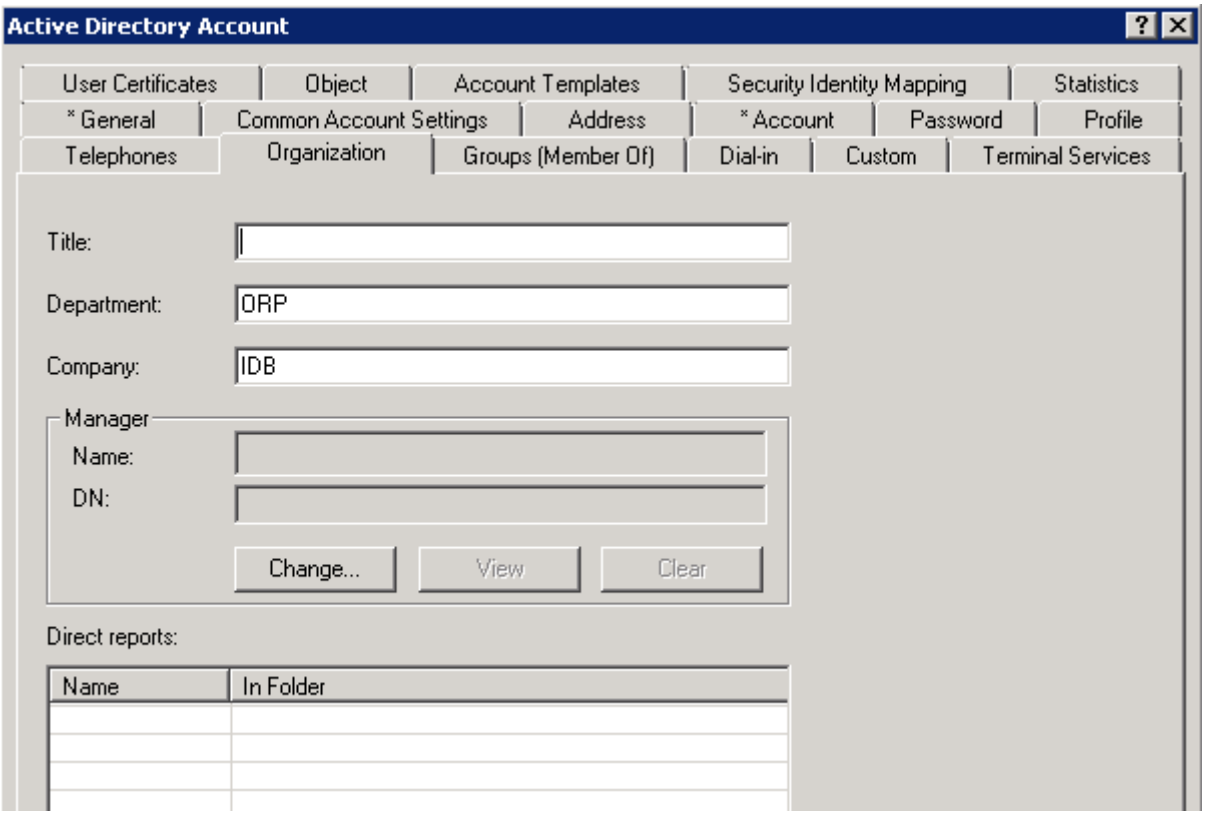


18.2.3 Transferir usuario

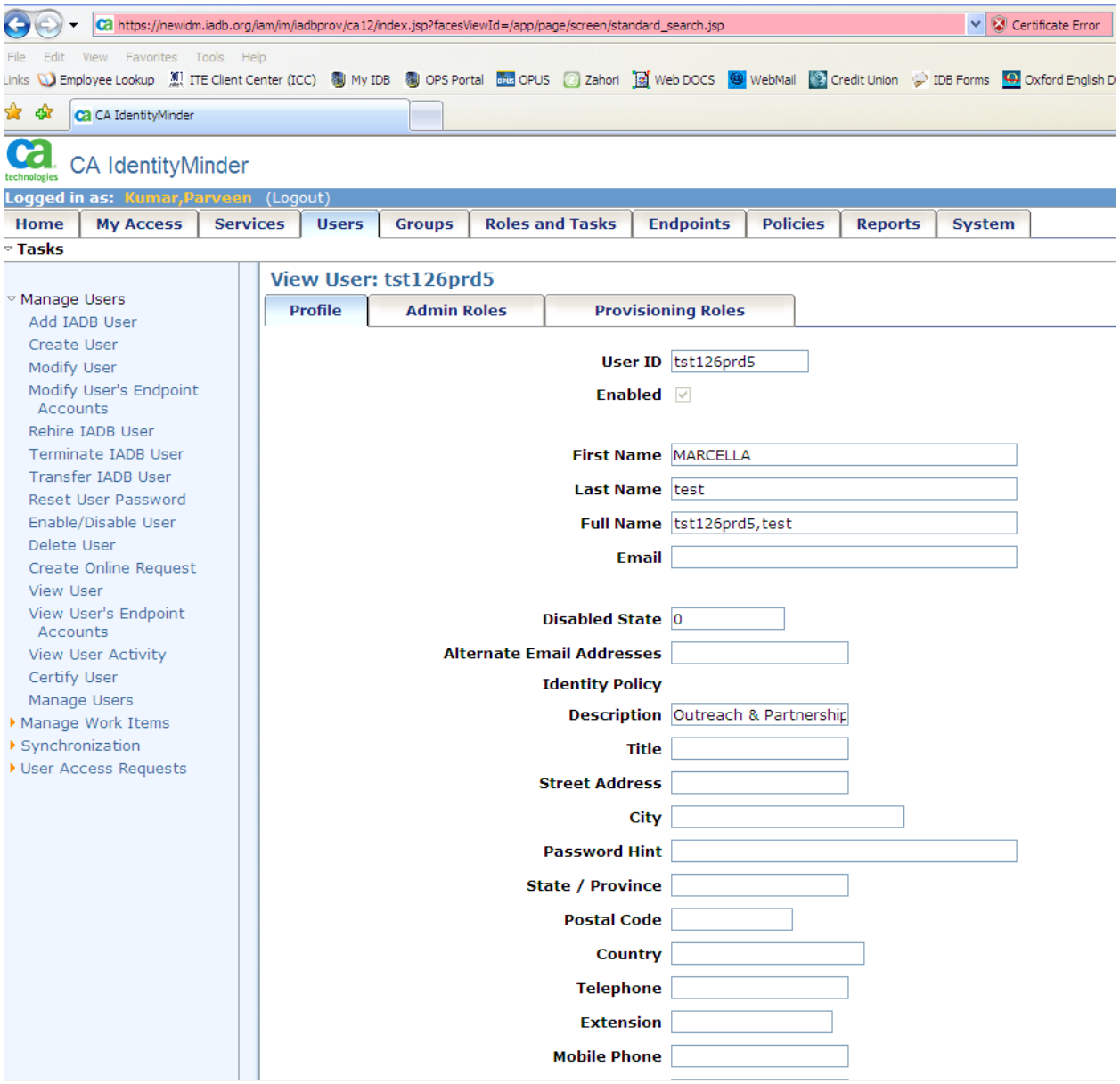
Continuar proceso para tranferir usuario

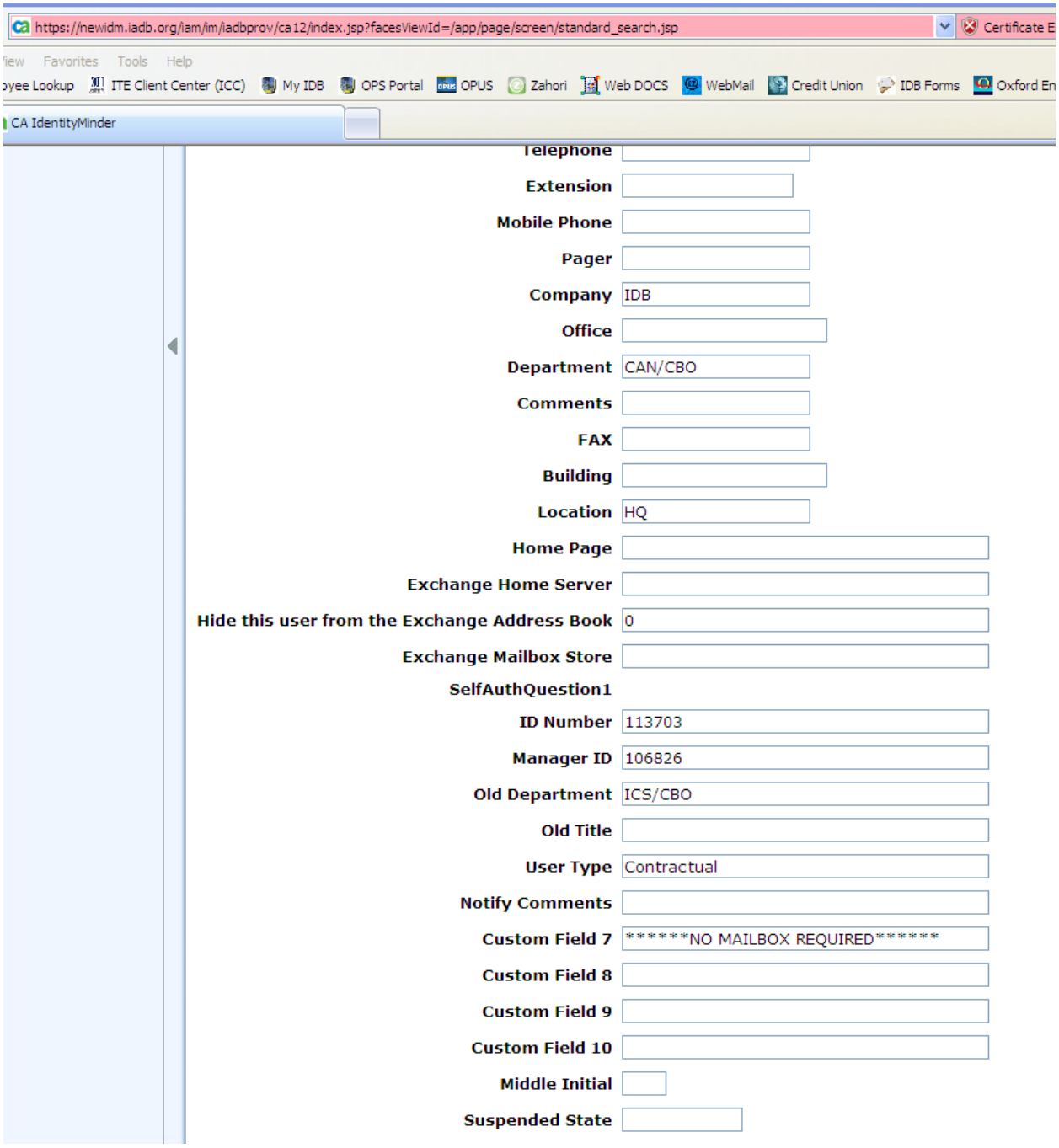

Global User
Workflow Security
Roles
Global Groups
ADS Domain Preference
Entrust PKI Domain Access
Statistics
* User
Password
Location
Custom Fields
SAWI/DAWI Admin
Admin Profiles
Administrative Privileges
Workflow
* Global user name:
tst126prd5
* Account name:
tst126prd5
First name:
MARCELLA
Middle name:
Last name:
test
Full name:
tst126prd5,test
Title:
Description:
Outreach & Partnerships
Company:
IDB
Department:
CAN/CBO
Comments:
Office:
Restricted user
Access status
Suspension state:
Active
Global User is not locked.
Unlock Global User
UID
Auto-generate
UID:
External time fields
Enable user:
12/ 5/2012
Delete user:
12/15/2012
Disable user:
9/17/2013
OK
Cancel
Apply


Global User
Workflow Security
Roles
Global Groups
ADS Domain Preference
Entrust PKI Domain Access
Statistics
* User
Password
Location
Custom Fields
SAWI/DAWI Admin
Admin Profiles
Administrative Privileges
Workflow
Field Name
*
ID
Value
Comment for Accounts ... 7 ******NO MAILBOX REQUIRED******
Department 3 ICS/CBO
Employee ID 1 113703
Manager ID 2
Rehired User Comments 6 Transfer User
Title 4
User Type 5 Contractor
Clear value...
Edit value...
Add value...
OK
Cancel
Apply


Active Directory Account
User Certificates
Object
Account Templates
Security Identity Mapping
Statistics
* General
Common Account Settings
Address
* Account
Password
Profile
Telephones
Organization
Groups (Member Of)
Dial-in
Custom
Terminal Services
Title:
Department:
ORP
Company:
IDB
Manager
Name:
DN:
Change...
View
Clear
Direct reports:
Name
In Folder

 187

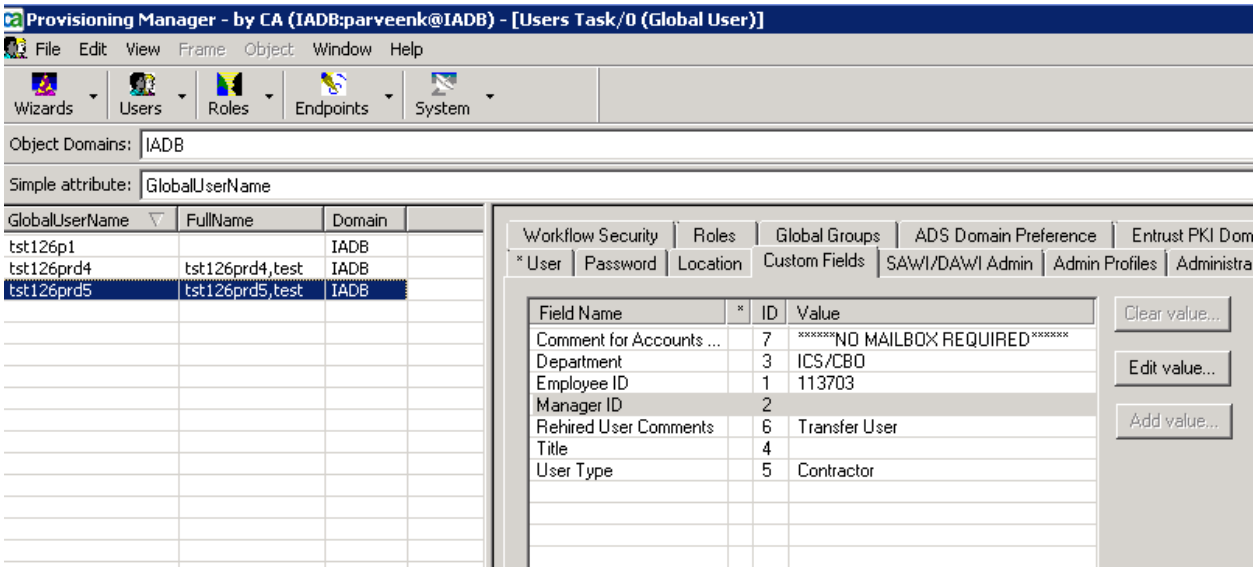

https://newidm.iadb.org/iam/im/iadbprov/ca12/index.jsp?facesViewId=/app/page/screen/standard_search.jsp
Certificate Error
File Edit View Favorites Tools Help
Links Employee Lookup ITE Client Center (ICC) My IDB OPS Portal OPUS Zahori Web DOCS WebMail Credit Union IDB Forms Oxford English D
CA IdentityMinder
CA IdentityMinder
Logged in as: Kumar,Parveen (Logout)
Home My Access Services Users Groups Roles and Tasks Endpoints Policies Reports System
Tasks
Manage Users
Add IADB User
Create User
Modify User
Modify User's Endpoint Accounts
Rehire IADB User
Terminate IADB User
Transfer IADB User
Reset User Password
Enable/Disable User
Delete User
Create Online Request
View User
View User's Endpoint Accounts
View User Activity
Certify User
Manage Users
Manage Work Items
Synchronization
User Access Requests
View User: tst126prd5
Profile
Admin Roles
Provisioning Roles
User ID tst126prd5
Enabled
First Name MARCELLA
Last Name test
Full Name tst126prd5,test
Email
Disabled State 0
Alternate Email Addresses
Identity Policy
Description Outreach & Partnership
Title
Street Address
City
Password Hint
State / Province
Postal Code
Country
Telephone
Extension
Mobile Phone



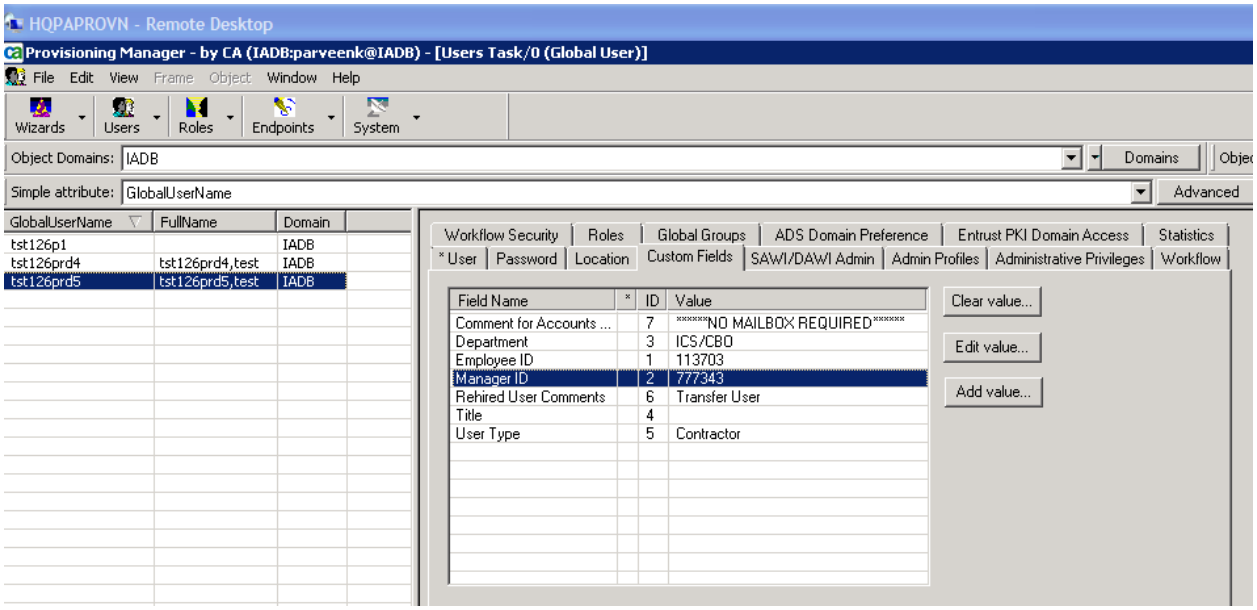
18.2.4 Actualización de usuario

Continue con el procesos para actualizaciones de usuarios globales para la identificacion del administrador.

Antes del cambio,



Despues del cambio,



19 Roles administrativos personalizados de Identity Minder

A continuacion se muestran los roles personalizados de administrador definidos para realizer diversas tareas.

- IADB Administrador del sistema
- IADB Administrador de usuarios
- IADB Oficial de seguridad
- IADB Auditor

Las reglas definidas para cada rol de administrador anteriormente son:

1. Administración de sistema:

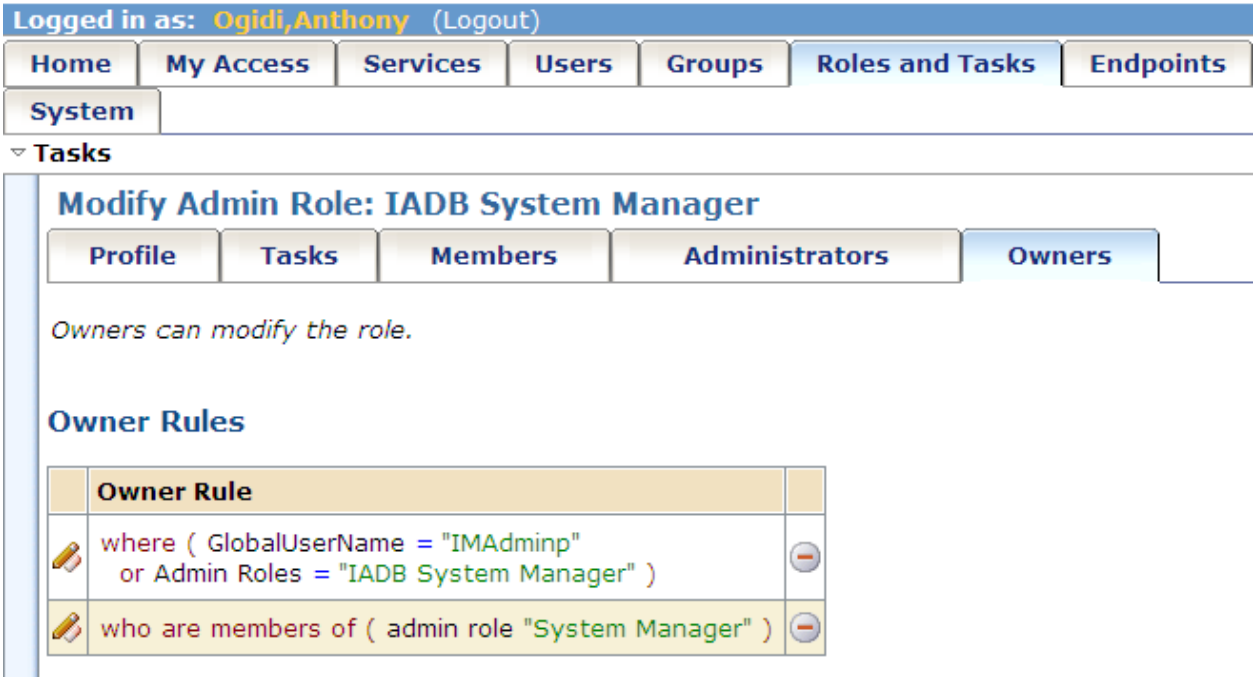
a. IADB Administrador de sistema- clon de la función SYSTEM MANAGER entregado : serán autorizados a conceder ningún papel aún BID SYSTEM MANAGER , SYSTEM MANAGER

i. Owner: IMAdmin id, IADB SYSTEM MANAGER, SYSTEM MANAGER

ii. Administrador: IADB administrador de sistema

iii. Member: IADB administrador de sistem

191


Logged in as: Ogidi,Anthony (Logout)
Home
My Access
Services
Users
Groups
Roles and Tasks
Endpoints
System
Tasks
Modify Admin Role: IADB System Manager
Profile
Tasks
Members
Administrators
Owners
Owners can modify the role.
Owner Rules
Owner Rule
where (GlobalUserName = "IMAdminp"
or Admin Roles = "IADB System Manager")
who are members of (admin role "System Manager")

192

Tasks

Modify Admin Role: IADB System Manager

Profile | Tasks | Members | Administrators | Owners

Administrators manage the members and administrators of this role.

Admin Policies

	Admin Rule	User Scope Rule	Manage Members	Manage Administrators	
	where (Admin Roles = "IADB System Manager" or Admin Roles = "System Manager")	(all)	☑	☑	⊖

Add

☑ **Administrators can add and remove administrators of this role**

Add Action

When a user is added as an administrator of this role, what changes occur?
(Changes must make the user meet an admin rule.)

Add IADB System Manager to Admin Roles ⊖

⊕

Remove Action

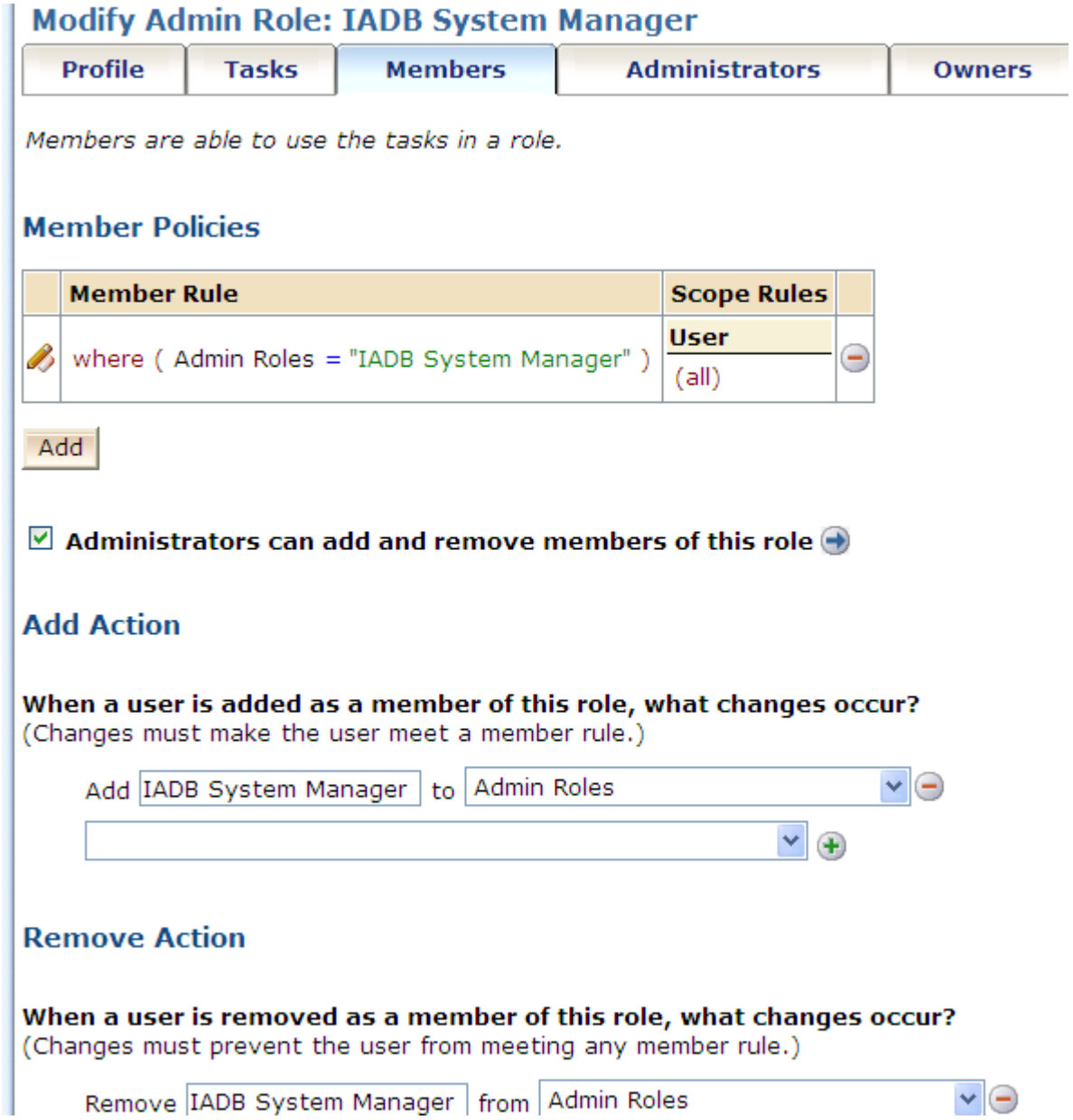
When a user is removed as an administrator of this role, what changes occur?
(Changes must prevent the user from meeting any admin rule.)

Remove IADB System Manager from Admin Roles ⊖

⊕

Copy admins from another role

Return to Search



2. Administrador de ususarios:

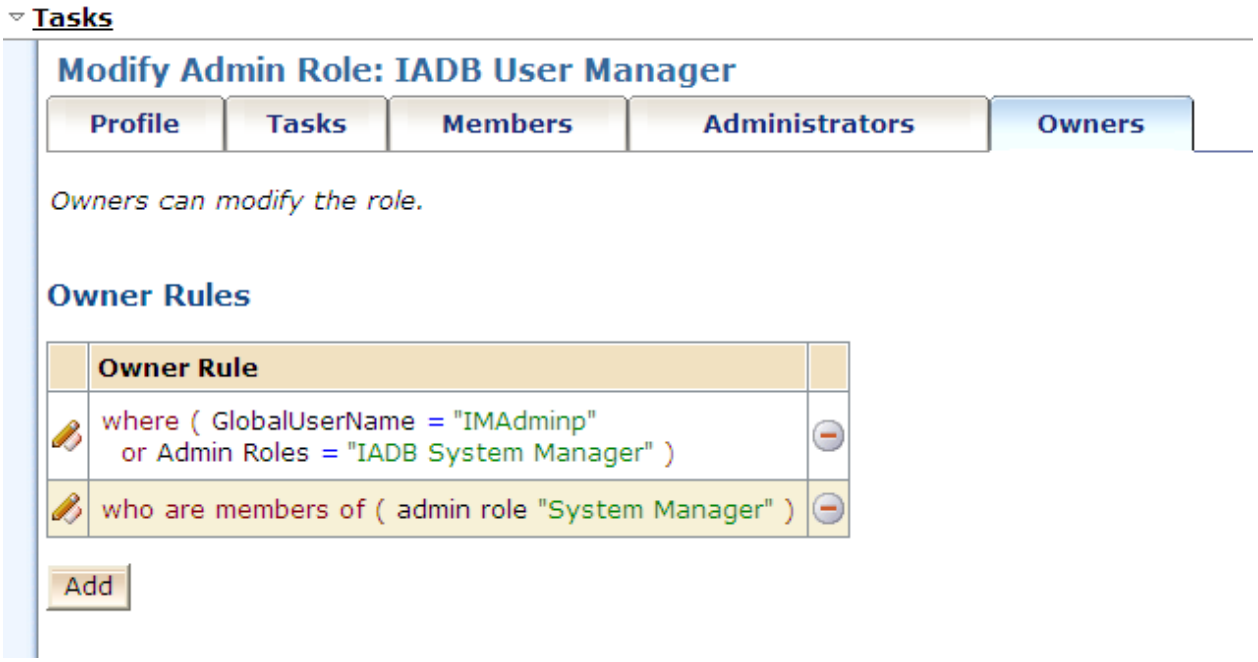
a. IADB Administrador de usuarios - clon de la función Administrador de usuarios entregado : serán autorizados a conceder ningún papel excepto BID Administrador de usuarios, Administrador de usuarios , BID

b. Administrador de sistema

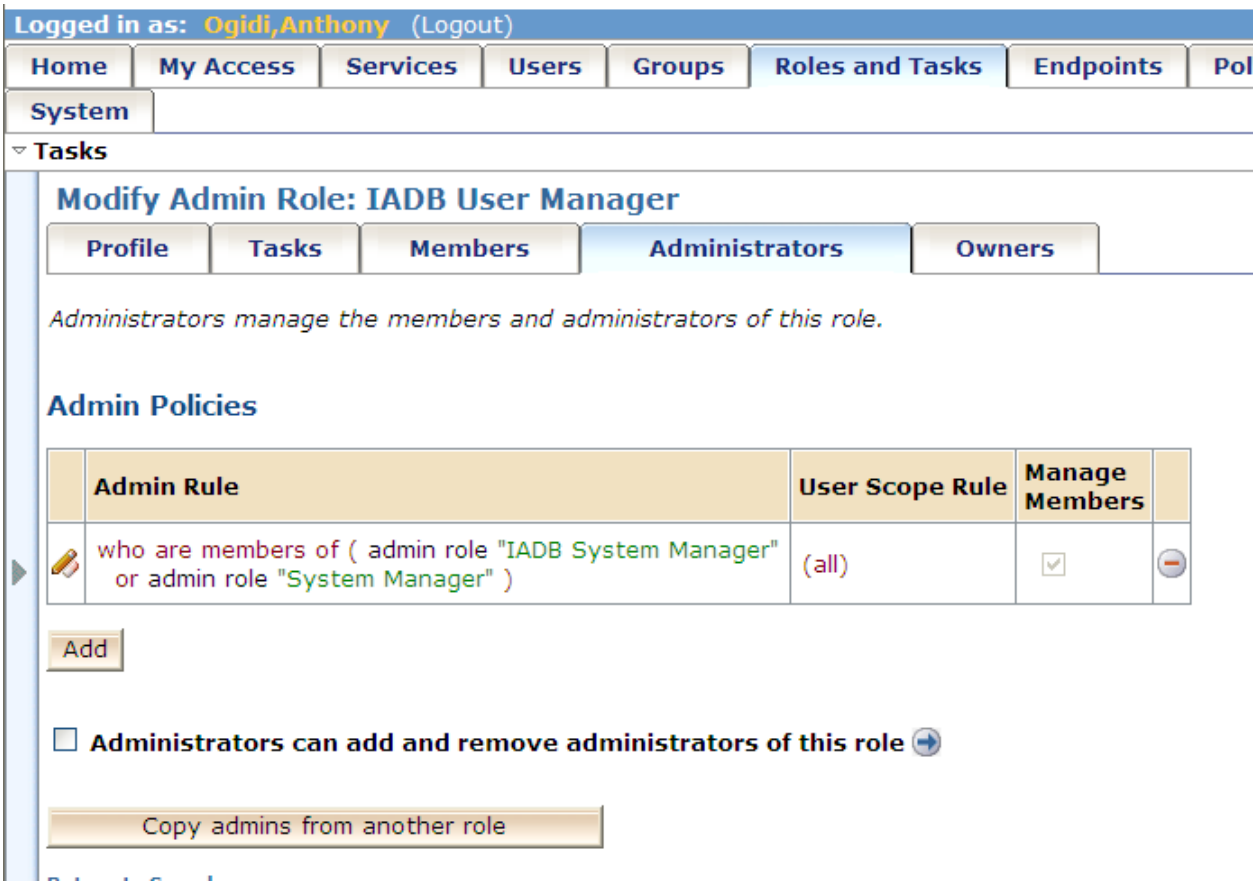
i. Propietarios: IMAdmin id, IADB administrador de usuarios, administrador de usuarios, IADB administrador de sistemas, administrador de sistemas

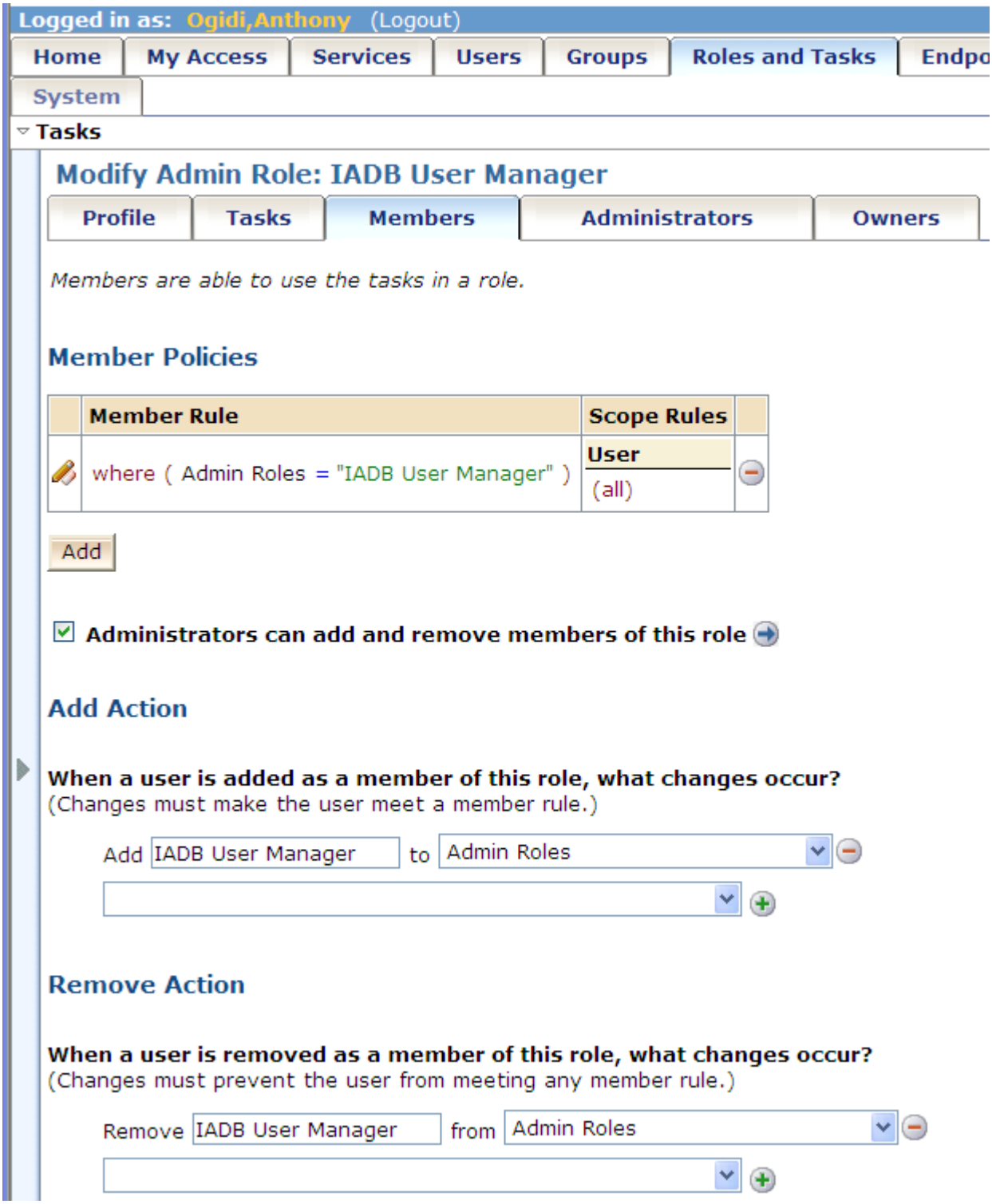
ii. Administrador: IADB administrador de usuarios, administrador de usuarios, IADB administrador de sistema, administrador de sistema

iii. Miembros: IADB administrador de usuarios, administrador de usuarios.



195


Logged in as: Ogidi,Anthony (Logout)
Home
My Access
Services
Users
Groups
Roles and Tasks
Endpoints
Pol
System
Tasks
Modify Admin Role: IADB User Manager
Profile
Tasks
Members
Administrators
Owners
Administrators manage the members and administrators of this role.
Admin Policies
Admin Rule
User Scope Rule
Manage Members
who are members of (admin role "IADB System Manager" or admin role "System Manager")
(all)
Add
Administrators can add and remove administrators of this role
Copy admins from another role



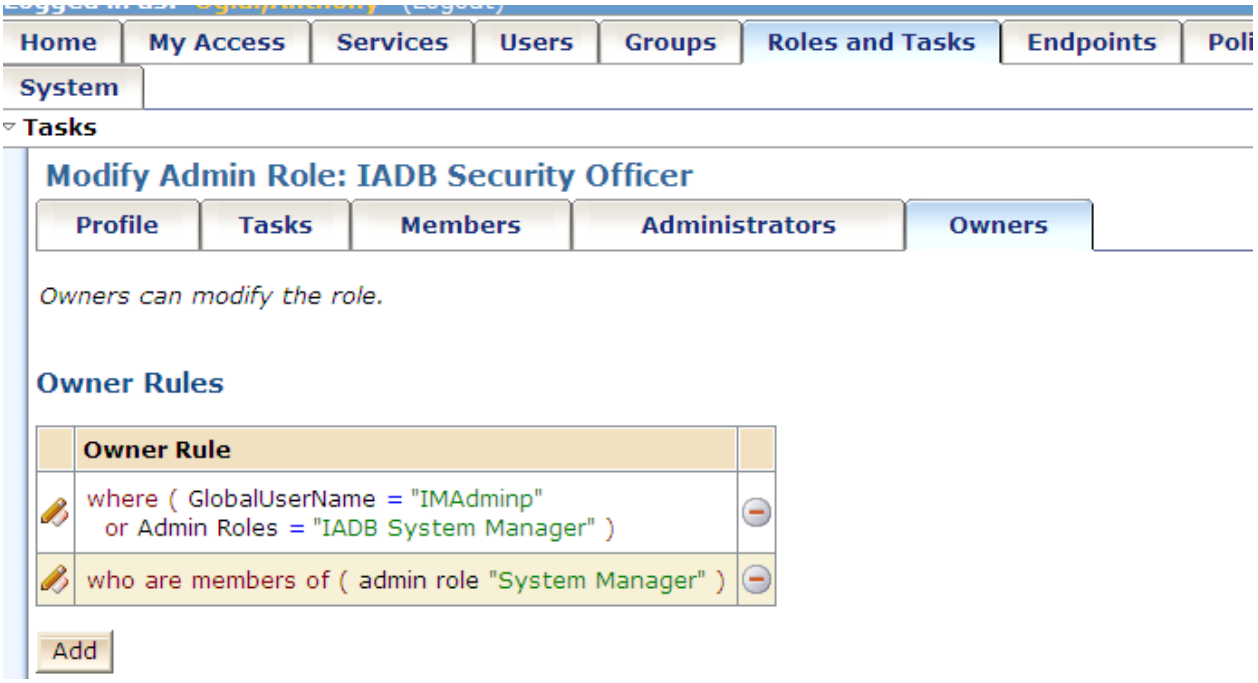
3. Oficial de Seguridad

a. IADB official de seguridad. - clon de la función Administrador de usuarios entregado : se autorizará para realizar la gestión de usuarios , pero no autorizado a conceder ningún papel .

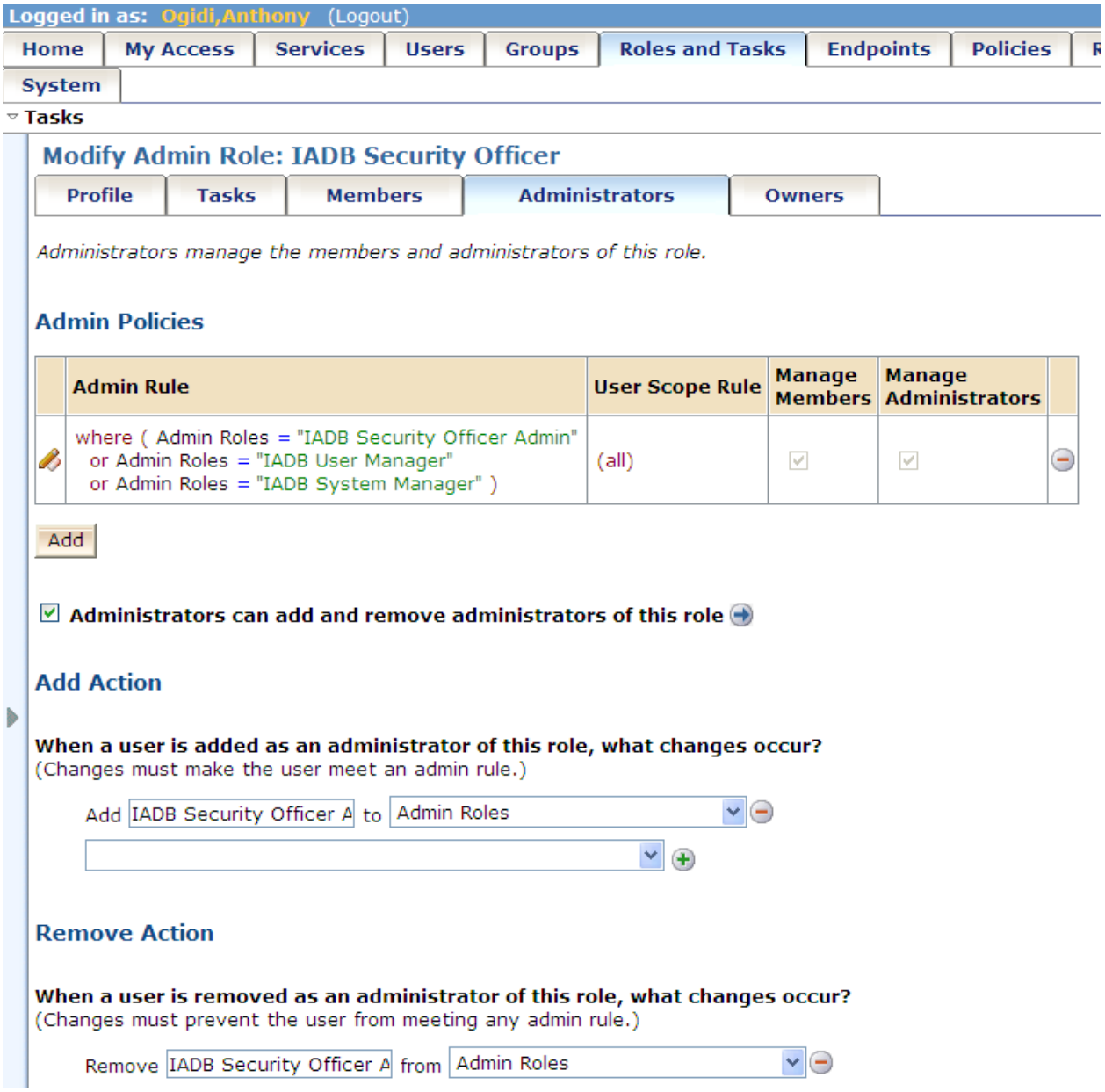
i. Propietarios: IMAdmin id, IADB Administrador de usuarios, Administrador de usuarios, IADB administrador de sistema, administrador de sistema

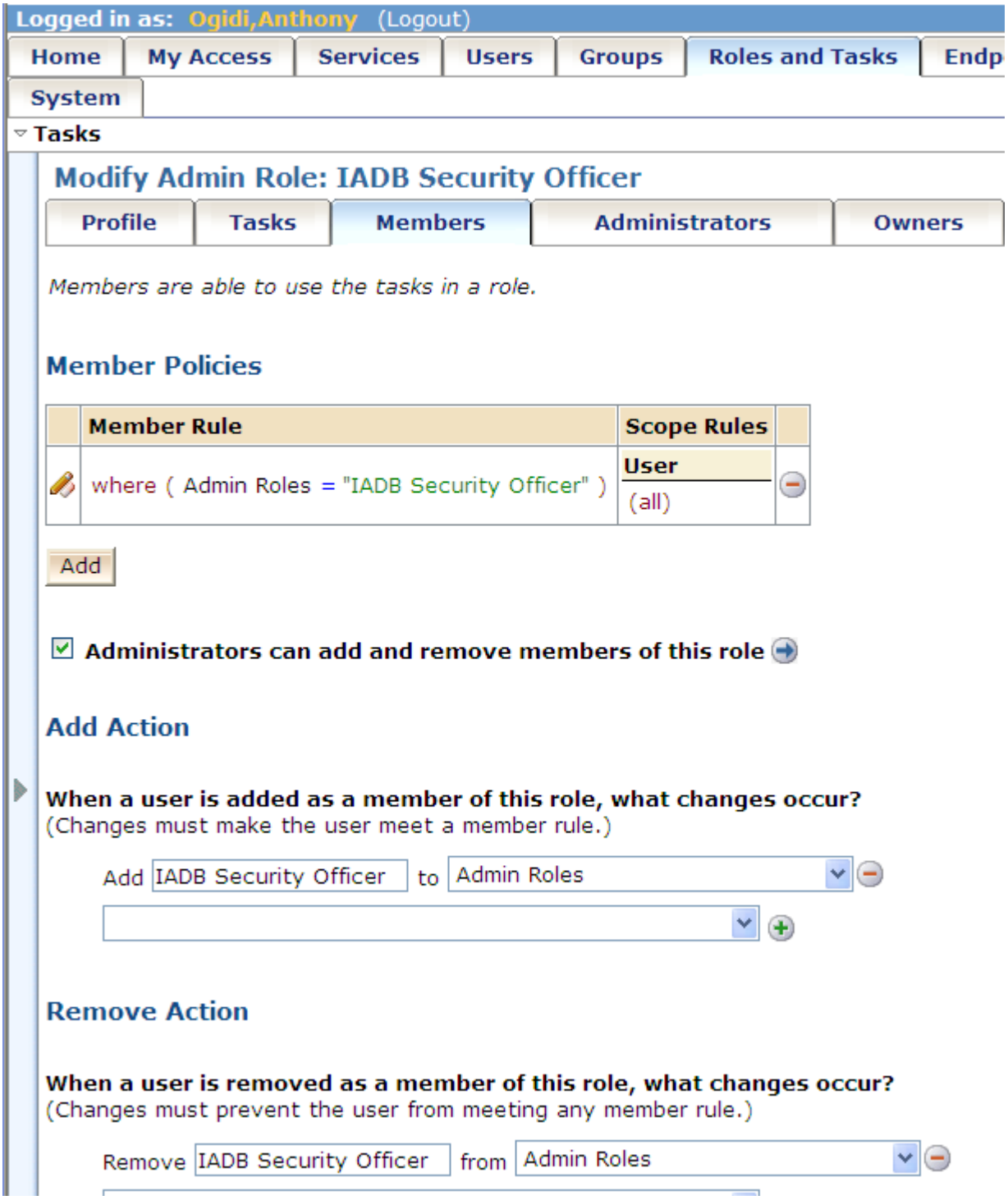
ii. Administrator: IADB Administrador de usuarios, Administrador de usuarios, IADB administrador de sistema, administrador de sistema

iii. Miembro: IADB oficial de seguridad



198


Logged in as: Ogidi,Anthony (Logout)
Home
My Access
Services
Users
Groups
Roles and Tasks
Endpoints
Policies
System
Tasks
Modify Admin Role: IADB Security Officer
Profile
Tasks
Members
Administrators
Owners
Administrators manage the members and administrators of this role.
Admin Policies
Admin Rule
User Scope Rule
Manage Members
Manage Administrators
where (Admin Roles = "IADB Security Officer Admin"
or Admin Roles = "IADB User Manager"
or Admin Roles = "IADB System Manager")
(all)
Add
Administrators can add and remove administrators of this role
Add Action
When a user is added as an administrator of this role, what changes occur?
(Changes must make the user meet an admin rule.)
Add IADB Security Officer A to Admin Roles
Remove Action
When a user is removed as an administrator of this role, what changes occur?
(Changes must prevent the user from meeting any admin rule.)
Remove IADB Security Officer A from Admin Roles



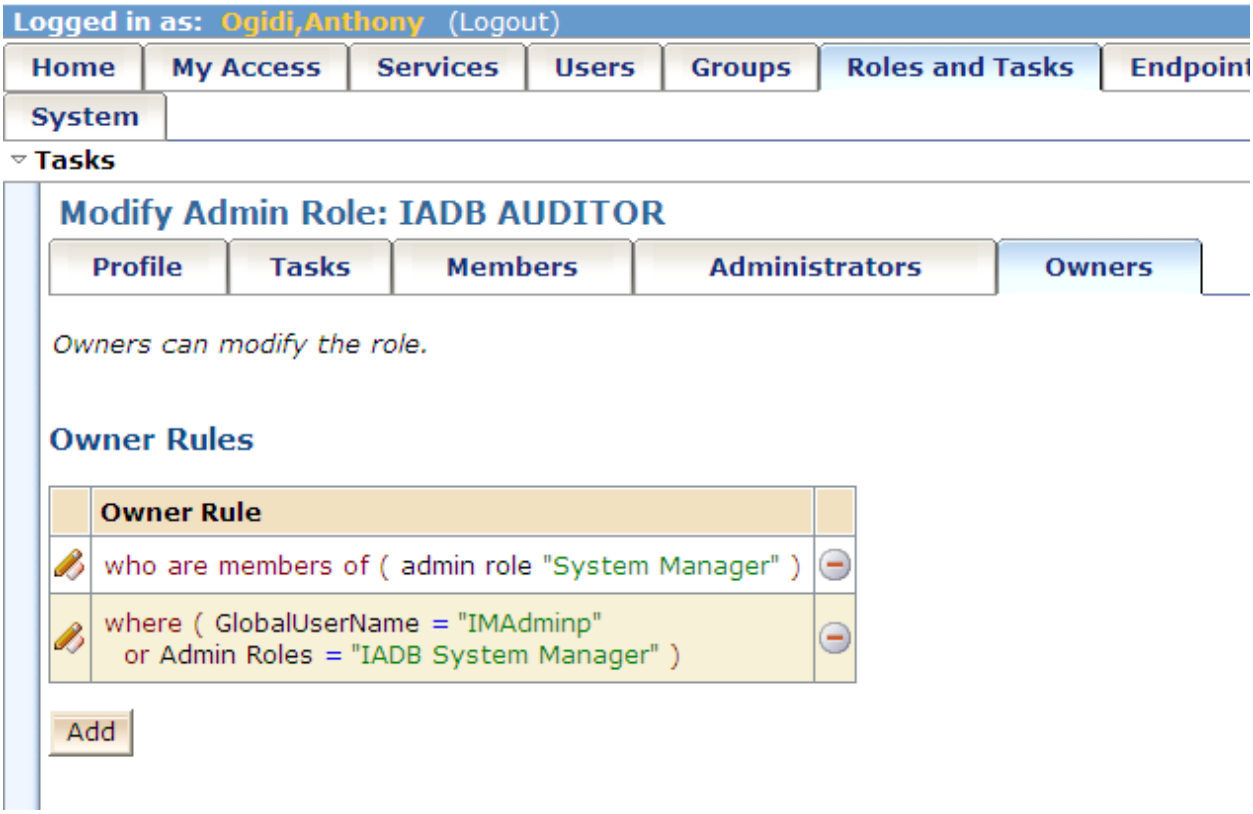
4. Auditor

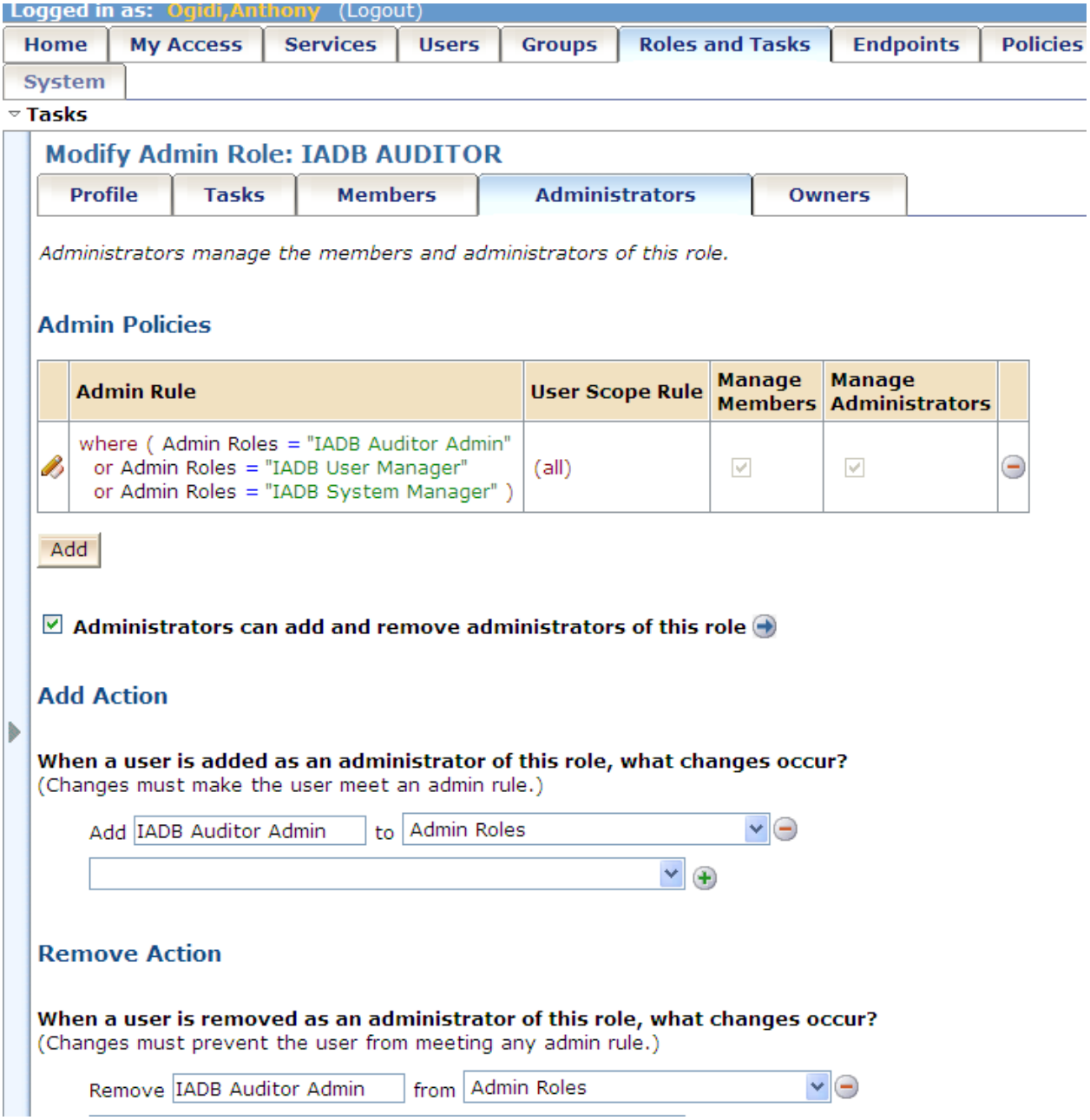
a. IADB AUDITOR- clone of the delivered AUDITOR role: Will be authorized to perform Auditing functions/reports but not authorized to grant any role.

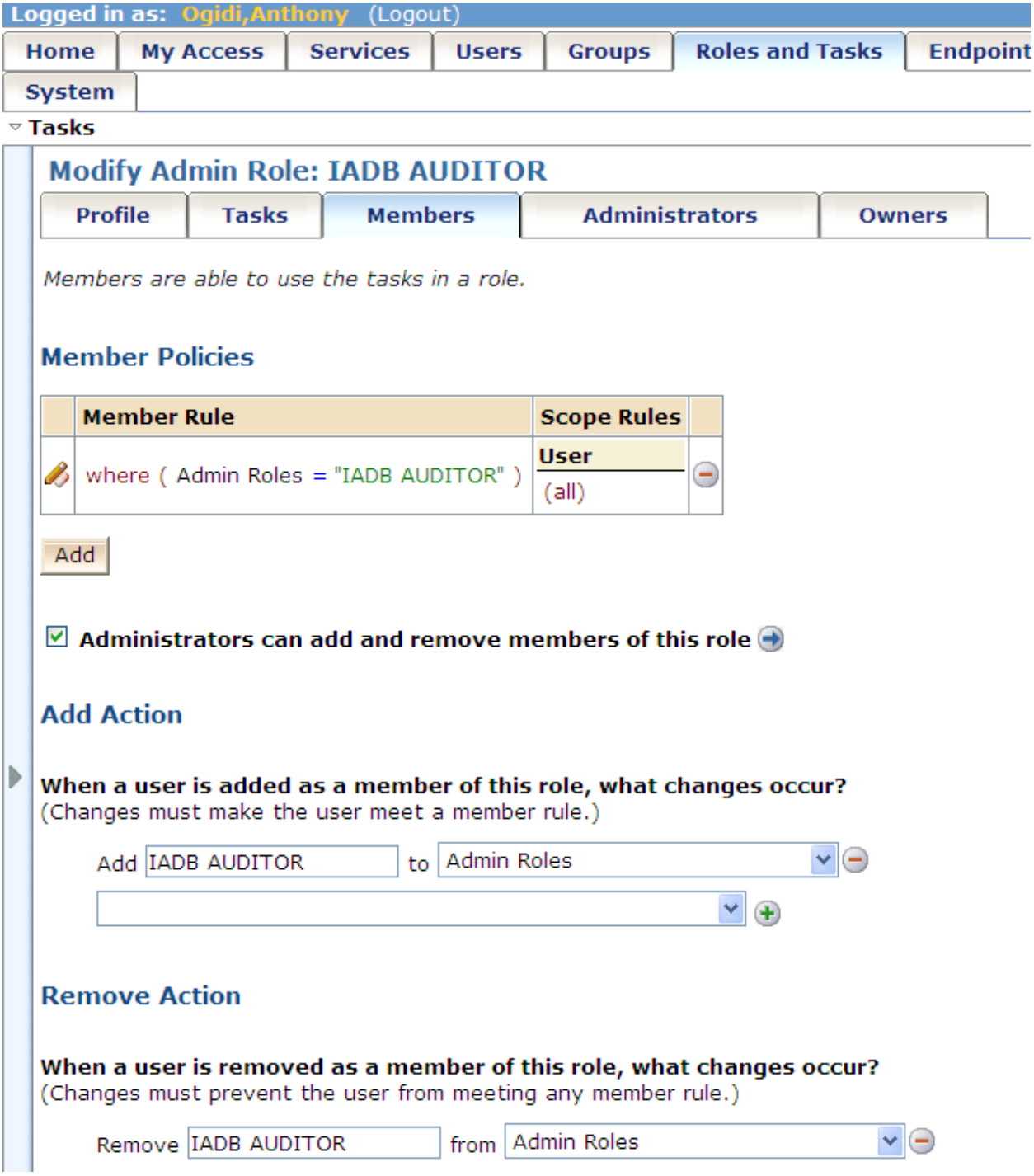
i. Owner: IMAdmin id, IADB USER MANAGER, USER MANAGER, IADB SYSTEM MANAGER, SYSTEM MANAGER

ii. Administrador: Administrador de usuarios BID, el Administrador de usuarios , BID SYSTEM MANAGER , SYSTEM MANAGER

iii. Member: IADB Oficial de seguridad




Logged in as: Ogidi,Anthony (Logout)
Home
My Access
Services
Users
Groups
Roles and Tasks
Endpoints
Policies
System
Tasks
Modify Admin Role: IADB AUDITOR
Profile
Tasks
Members
Administrators
Owners
Administrators manage the members and administrators of this role.
Admin Policies
Admin Rule
User Scope Rule
Manage Members
Manage Administrators
where (Admin Roles = "IADB Auditor Admin"
or Admin Roles = "IADB User Manager"
or Admin Roles = "IADB System Manager")
(all)
Add
Administrators can add and remove administrators of this role
Add Action
When a user is added as an administrator of this role, what changes occur?
(Changes must make the user meet an admin rule.)
Add IADB Auditor Admin to Admin Roles
Remove Action
When a user is removed as an administrator of this role, what changes occur?
(Changes must prevent the user from meeting any admin rule.)
Remove IADB Auditor Admin from Admin Roles

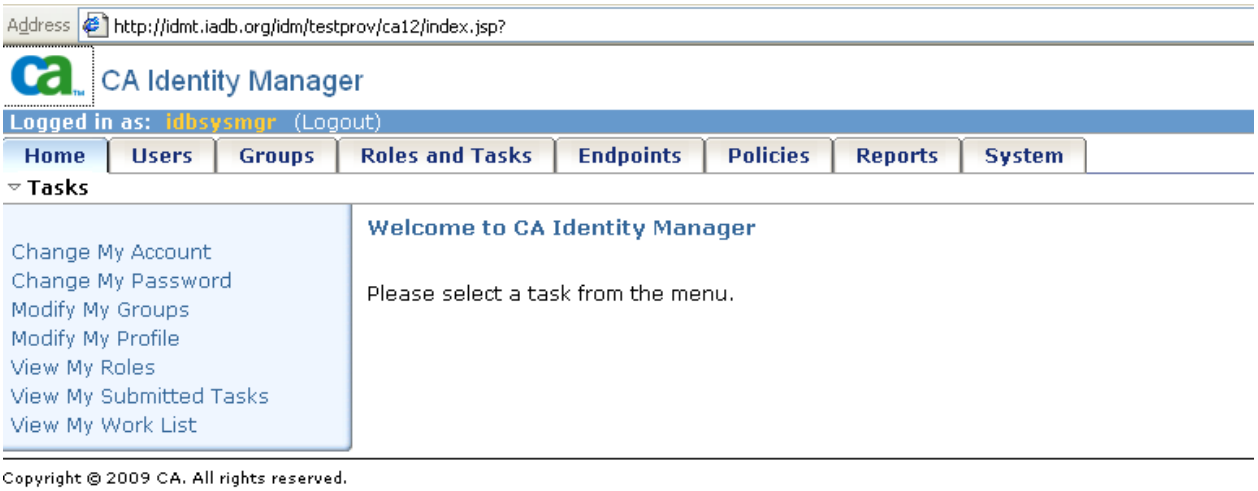


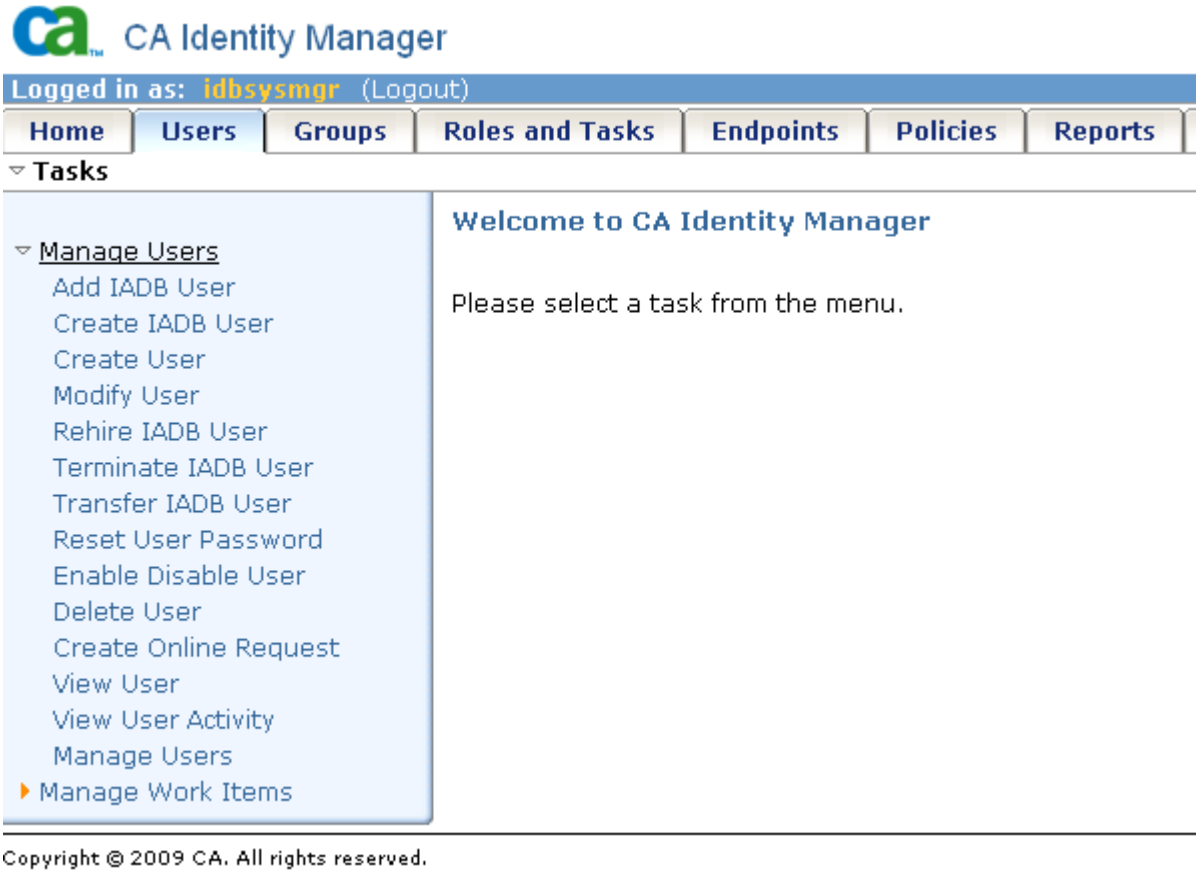
19.1 IADB Administrador de sistema

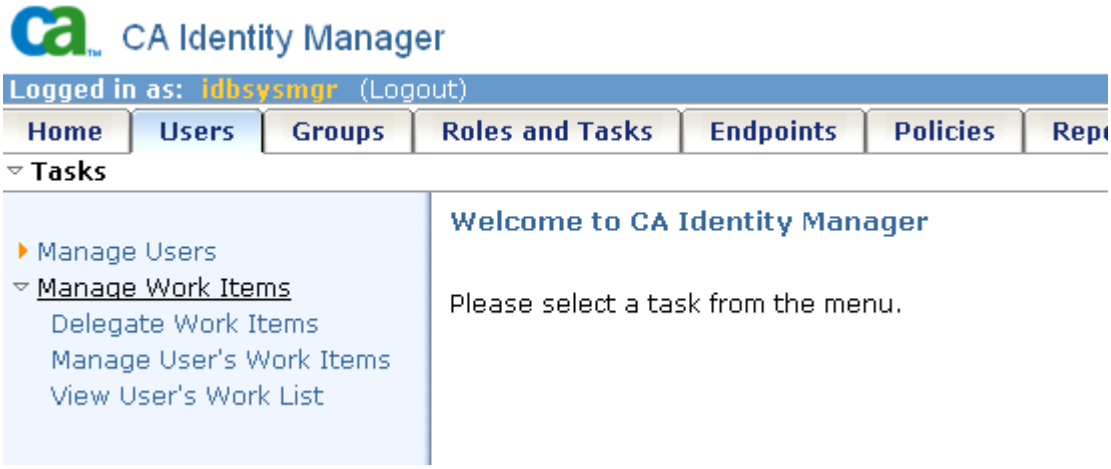
Los miembros de este rol son los súper usuarios para gestionar / administrar Identidad Minder . Ellos son los dueños de todas las tareas de administración y tienen la capacidad de crear / modificar / eliminar las tareas de administración. Los miembros de este rol podrán ver la mayora de las tareas

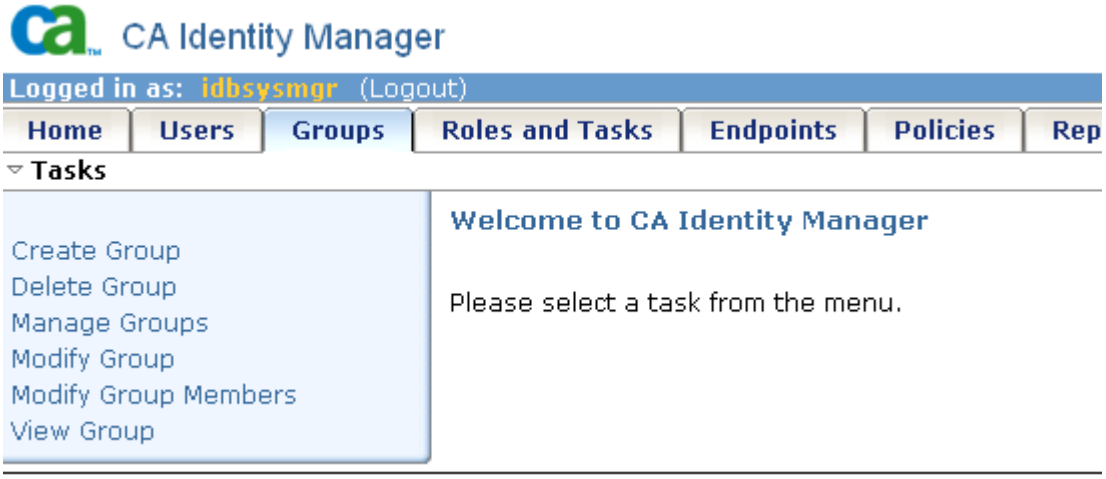
de administración de forma predeterminada. Sin embargo , sólo pueden ver las tareas de administración de encargo si cumplen la regla miembro se define en las tareas.

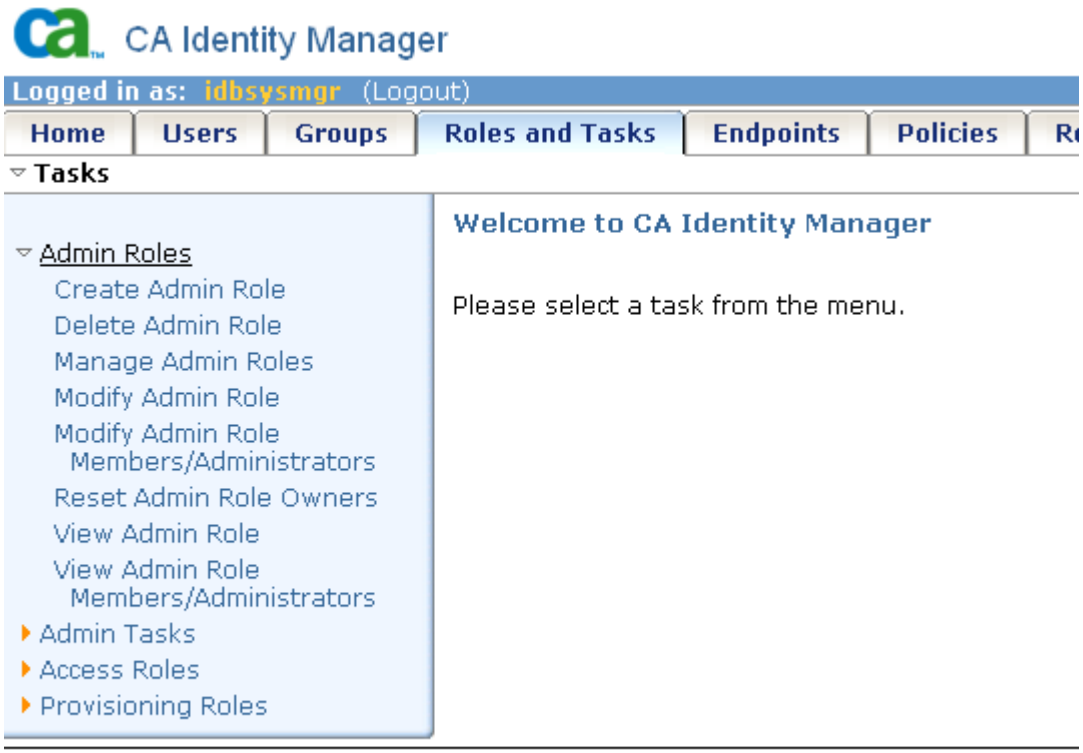
A continuación se muestra las imágenes de las tareas BID Administrador de sistema.

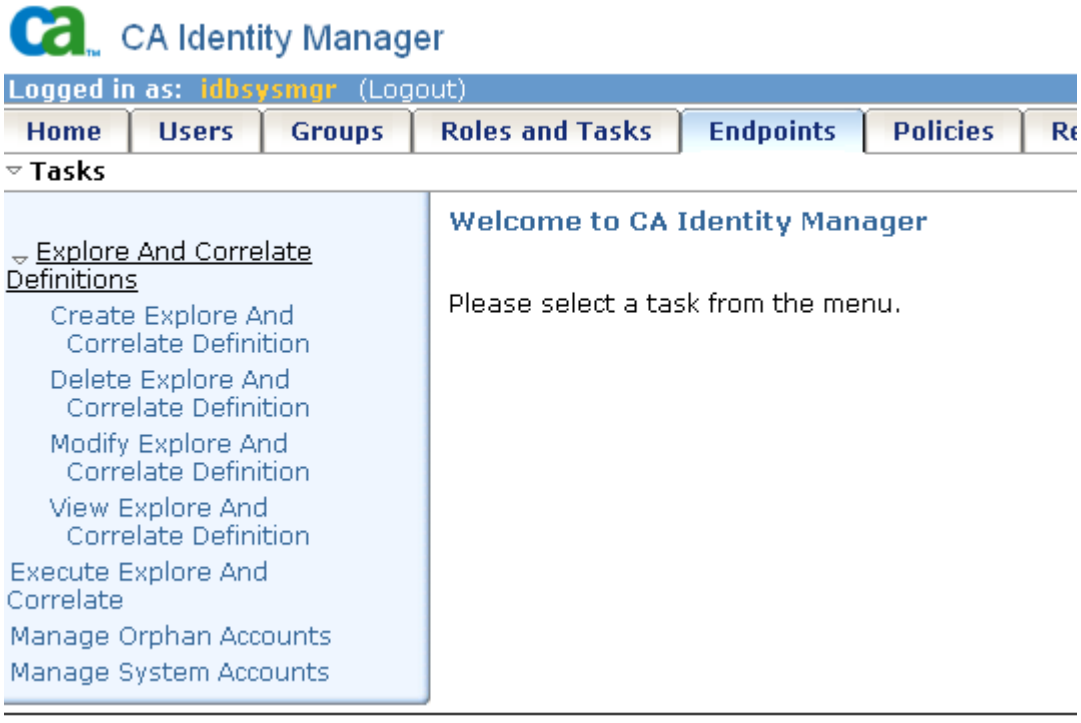


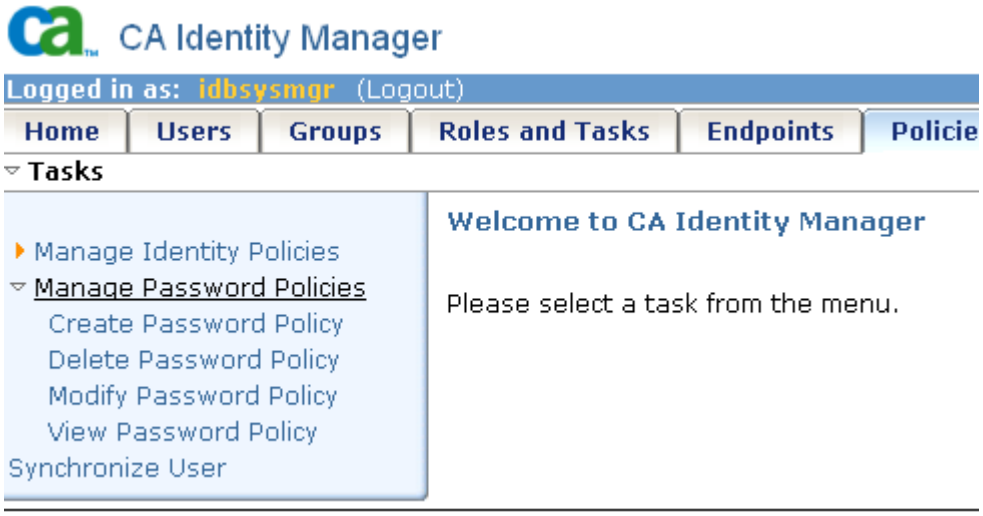


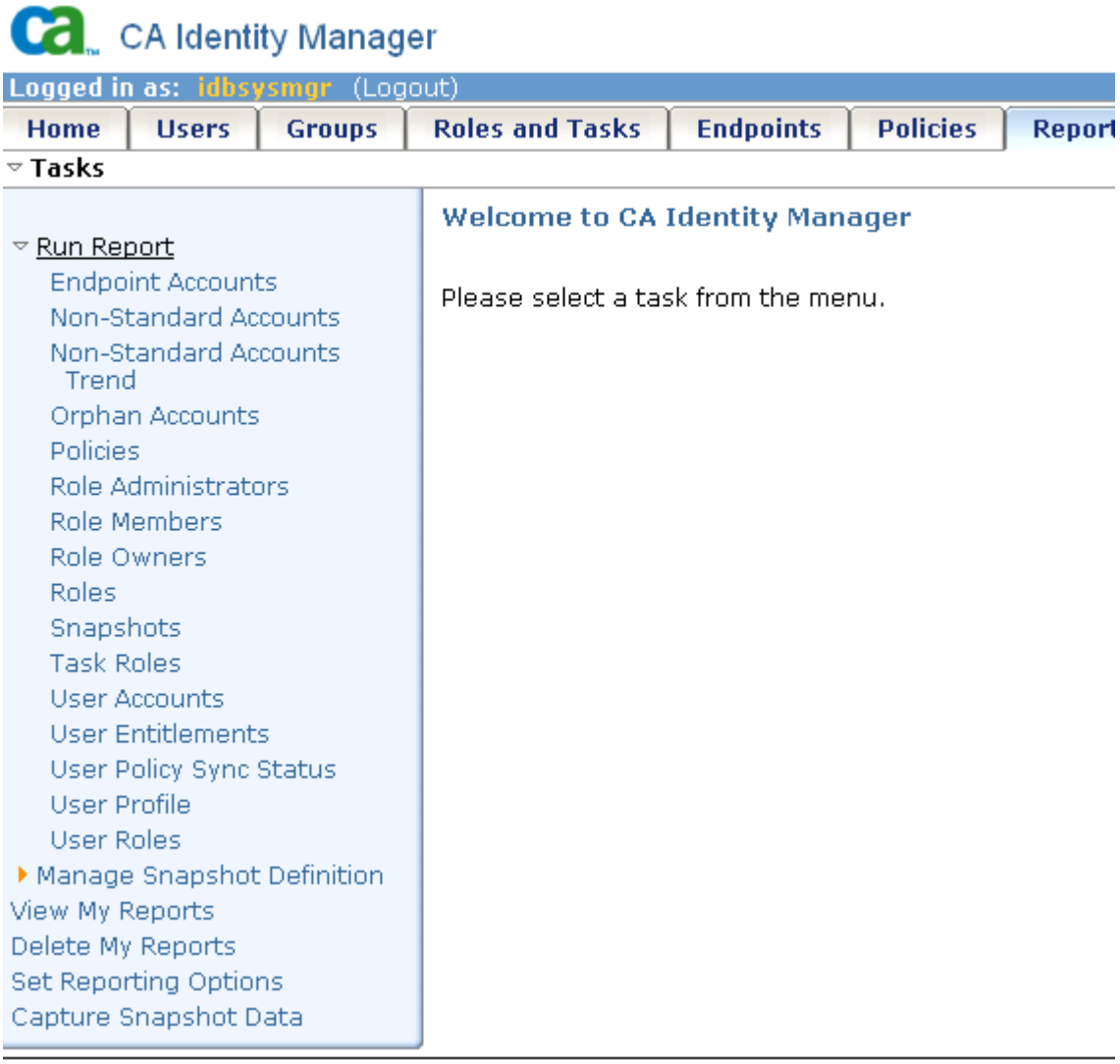

CA Identity Manager
Logged in as: idbsysmgr (Logout)
Home
Users
Groups
Roles and Tasks
Endpoints
Policies
Rep
Tasks
Manage Users
Manage Work Items
Delegate Work Items
Manage User's Work Items
View User's Work List
Welcome to CA Identity Manager
Please select a task from the menu.

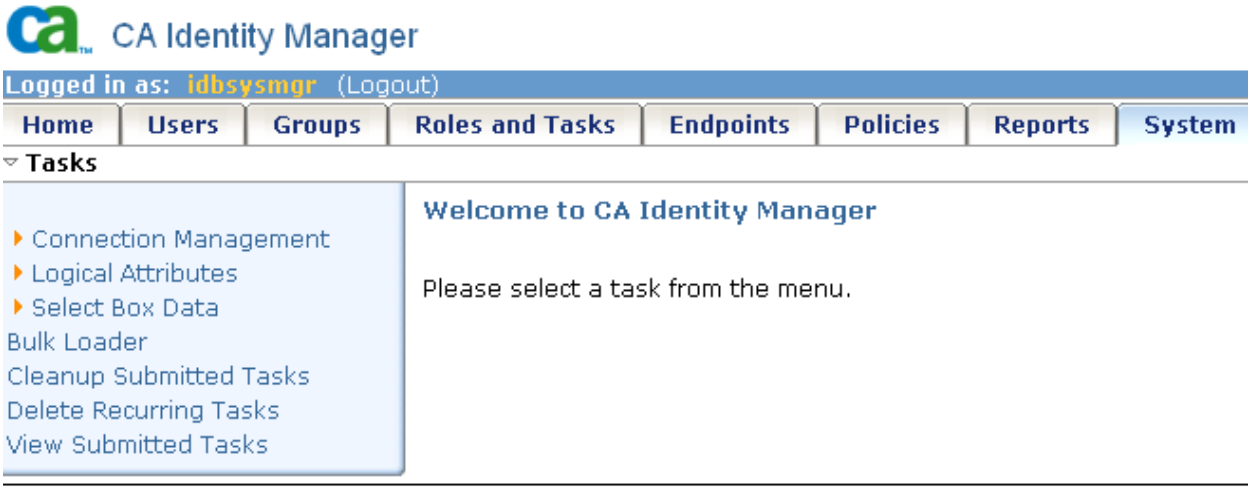

CA Identity Manager
Logged in as: idbsysmgr (Logout)
Home
Users
Groups
Roles and Tasks
Endpoints
Policies
Rep
Tasks
Create Group
Delete Group
Manage Groups
Modify Group
Modify Group Members
View Group
Welcome to CA Identity Manager
Please select a task from the menu.


CA Identity Manager
Logged in as: idbsysmgr (Logout)
Home
Users
Groups
Roles and Tasks
Endpoints
Policies
Tasks
Admin Roles
Create Admin Role
Delete Admin Role
Manage Admin Roles
Modify Admin Role
Modify Admin Role Members/Administrators
Reset Admin Role Owners
View Admin Role
View Admin Role Members/Administrators
Admin Tasks
Access Roles
Provisioning Roles
Welcome to CA Identity Manager
Please select a task from the menu.
Copyright © 2009 CA. All rights reserved.


CA Identity Manager
Logged in as: idbsysmgr (Logout)
Home
Users
Groups
Roles and Tasks
Endpoints
Policies
Tasks
Explore And Correlate Definitions
Create Explore And Correlate Definition
Delete Explore And Correlate Definition
Modify Explore And Correlate Definition
View Explore And Correlate Definition
Execute Explore And Correlate
Manage Orphan Accounts
Manage System Accounts
Welcome to CA Identity Manager
Please select a task from the menu.


CA Identity Manager
Logged in as: idbsysmgr (Logout)
Home
Users
Groups
Roles and Tasks
Endpoints
Policie
Tasks
Manage Identity Policies
Manage Password Policies
Create Password Policy
Delete Password Policy
Modify Password Policy
View Password Policy
Synchronize User
Welcome to CA Identity Manager
Please select a task from the menu.


CA Identity Manager
Logged in as: idbsysmgr (Logout)
Home
Users
Groups
Roles and Tasks
Endpoints
Policies
Report
Tasks
Run Report
Endpoint Accounts
Non-Standard Accounts
Non-Standard Accounts Trend
Orphan Accounts
Policies
Role Administrators
Role Members
Role Owners
Roles
Snapshots
Task Roles
User Accounts
User Entitlements
User Policy Sync Status
User Profile
User Roles
Manage Snapshot Definition
View My Reports
Delete My Reports
Set Reporting Options
Capture Snapshot Data
Welcome to CA Identity Manager
Please select a task from the menu.


CA Identity Manager
Logged in as: idbsysmgr (Logout)
Home
Users
Groups
Roles and Tasks
Endpoints
Policies
Reports
System
Tasks
Connection Management
Logical Attributes
Select Box Data
Bulk Loader
Cleanup Submitted Tasks
Delete Recurring Tasks
View Submitted Tasks
Welcome to CA Identity Manager
Please select a task from the menu.

19.2 IADB Administrador de usuario

A continuación se presentan las tareas de administración asignados a la función BID Administrador de usuarios.

View Admin Role: *IADB User Manager*

Profile | Tasks | Members | Administrators | Owners

Select tasks for the role.

1 2 ›

Task	Description	Category	Primary Object
Modify Group Members		Groups	Group
View My Roles		Home	User
View My Submitted Tasks		Home	User
View My Work List		Home	User
Capture Snapshot Data		Reports	None
Create Snapshot Definition		Reports	Snapshot Type
Delete My Reports		Reports	Report Instance
Delete Snapshot Definition		Reports	Snapshot Type
Endpoint Accounts	Endpoint Accounts	Reports	Report Instance
Modify Snapshot Definition		Reports	Snapshot Type
Non-Standard Accounts	Non-Standard Accounts	Reports	Report Instance
Non-Standard Accounts Trend	Non-Standard Accounts Trend	Reports	Report Instance
Orphan Accounts	Orphan Accounts	Reports	Report Instance
Policies	Policies	Reports	Report Instance
Role Administrators	Role Administrators	Reports	Report Instance
Role Members	Role Members	Reports	Report Instance
Role Owners	Role Owners	Reports	Report Instance
Roles	Roles	Reports	Report Instance
Snapshots	Snapshots	Reports	Report Instance
Task Roles	Task Roles	Reports	Report Instance
User Accounts	User Accounts	Reports	Report Instance
User Entitlements	User Entitlements	Reports	Report Instance
User Policy Sync Status	User Policy Sync Status	Reports	Report Instance
User Profile	User Profile	Reports	Report Instance
User Roles	User Roles	Reports	Report Instance
View My Reports		Reports	Report Instance
View Snapshot Definition		Reports	Snapshot Type
Modify Access Role Members/Administrators		Roles and Tasks	Access Role
Modify Provisioning Role Members/Administrators		Roles and Tasks	Provisioning Role
View Access Role Members/Administrators		Roles and Tasks	Access Role
View Admin Role		Roles and Tasks	Admin Role
View Admin Role Members/Administrators		Roles and Tasks	Admin Role
View Provisioning Role Members/Administrators		Roles and Tasks	Provisioning Role
Add IADB User		Users	User
Approve Accumulated Provisioning Roles		Users	None
Approve Create User		Users	User
Approve Delete User		Users	User
Approve Modify User		Users	User
Approve Online Request		Users	User
Certify User		Users	User
Create IADB User	No notification	Users	User

209

Create Online Request		Users	User
Create User		Users	User
Delegate Work Items		Users	User
Delete User		Users	User
Enable Disable User		Users	User
Implement Online Request		Users	User
Manage User's Work Items		Users	User
Manage Users		Users	User
Modify User		Users	User

1 2 ›

Select tasks for the role.

‹ 1 2

Task	Description	Category	Primary Object
Rehire IADB User		Users	User
Reset User Password		Users	User
Terminate IADB User		Users	User
Transfer IADB User		Users	User
View User		Users	User
View User's Work List		Users	User
View User Activity		Users	User

‹ 1 2

19.3 IADB Auditor

A continuación están las tareas de administración asignadas a papel Auditor BID

Tasks

View Admin Role: *IADB AUDITOR*

Profile | Tasks | Members | Administrators | Owners

Select tasks for the role.

Task	Description	Category	Primary Object
Non-Standard Accounts	Non-Standard Accounts	Reports	Report Instance
Policies	Policies	Reports	Report Instance
Role Administrators	Role Administrators	Reports	Report Instance
Task Roles	Task Roles	Reports	Report Instance
User Accounts	User Accounts	Reports	Report Instance
User Entitlements	User Entitlements	Reports	Report Instance
User Policy Sync Status	User Policy Sync Status	Reports	Report Instance
User Profile	User Profile	Reports	Report Instance
User Roles	User Roles	Reports	Report Instance
View My Reports		Reports	Report Instance
View Snapshot Definition		Reports	Snapshot Type
View Submitted Tasks		System	None

19.4 IADB Oficial de seguridad

A continuación se presentan las tareas de administración asignadas a la función oficial de seguridad del BID

211

View Admin Role: *IADB Security Officer*

Profile | Tasks | Members | Administrators | Owners

Select tasks for the role.

Task	Description	Category	Primary Object
Modify Group Members		Groups	Group
View My Roles		Home	User
View My Submitted Tasks		Home	User
View My Work List		Home	User
Create Snapshot Definition		Reports	Snapshot Type
Delete My Reports		Reports	Report Instance
Delete Snapshot Definition		Reports	Snapshot Type
Endpoint Accounts	Endpoint Accounts	Reports	Report Instance
Modify Snapshot Definition		Reports	Snapshot Type
Non-Standard Accounts	Non-Standard Accounts	Reports	Report Instance
Non-Standard Accounts Trend	Non-Standard Accounts Trend	Reports	Report Instance
Orphan Accounts	Orphan Accounts	Reports	Report Instance
Policies	Policies	Reports	Report Instance
Role Administrators	Role Administrators	Reports	Report Instance
Role Members	Role Members	Reports	Report Instance
Role Owners	Role Owners	Reports	Report Instance
Roles	Roles	Reports	Report Instance
Snapshots	Snapshots	Reports	Report Instance
Task Roles	Task Roles	Reports	Report Instance
User Accounts	User Accounts	Reports	Report Instance
User Entitlements	User Entitlements	Reports	Report Instance
User Policy Sync Status	User Policy Sync Status	Reports	Report Instance
User Profile	User Profile	Reports	Report Instance
User Roles	User Roles	Reports	Report Instance
View My Reports		Reports	Report Instance
View Snapshot Definition		Reports	Snapshot Type
Modify Access Role Members/Administrators		Roles and Tasks	Access Role
Modify Provisioning Role Members/Administrators		Roles and Tasks	Provisioning Role
View Access Role Members/Administrators		Roles and Tasks	Access Role
View Provisioning Role Members/Administrators		Roles and Tasks	Provisioning Role
Add IADB User		Users	User
Create IADB User	No notification	Users	User
Delegate Work Items		Users	User
Delete User		Users	User
Manage User's Work Items		Users	User
Manage Users		Users	User
Modify User		Users	User
Rehire IADB User		Users	User
Terminate IADB User		Users	User
Transfer IADB User		Users	User
View User		Users	User
View User's Work List		Users	User

212

20 Perfiles de abastecimiento de administracion de servicio

Perfiles de administrador permiten administradores ciertos tipos de acceso y privilegios para administrar objetos en un dominio. Perfiles admin contienen todos los privilegios que los administradores necesitan para realizar diferentes tareas .

20.1 Perfiles de administrador por defecto

■ Administrador de dominio - proporciona a los administradores acceso completo a todos los objetos en el dominio. Los administradores que tienen este perfil en el dominio raíz tienen acceso completo a todos los objetos Provisioning Server y la información de seguridad.

'etaadmin' es el administrador de dominio para el entorno de producción

Y "imadmintest" es el administrador de dominio para el entorno de prueba

■ Contraseña administrador- Permite a los administradores cambiar contraseñas y activar o suspender los usuarios globales.

■ UserAdministrator- Le permite a los administradores gestionar los usuarios en el dominio. Los administradores con este perfil no puede modificar el aprovisionamiento de roles o plantillas de cuenta.

■ ReadAdministrator- Permite a los administradores leer todos los objetos del dominio.

■ SelfAdministrator- Define las acciones que se pueden realizar por selfadministrators. Por defecto, este perfil autoriza auto-administración de leer su propio objeto de usuario global, una lista de sus cuentas, y modificar atributos específicos de su cuenta de usuario o cuentas global. Puede personalizar este perfil para satisfacer sus requisitos de autorización de auto-administrador.

Nota: Con la excepción de SelfAdministrator, no se puede modificar o eliminar estos perfiles.

Perfiles personalizados Provisioning admin

SQAREADadministrator

SQASECURITYOFFICER

213

21 Codigo personalizado JAVA

Hay dos clases de Java personalizado utilizados en el despliegue

- UserProfileHandler
- ModifyUserListener

21.1 UserProfileHandler

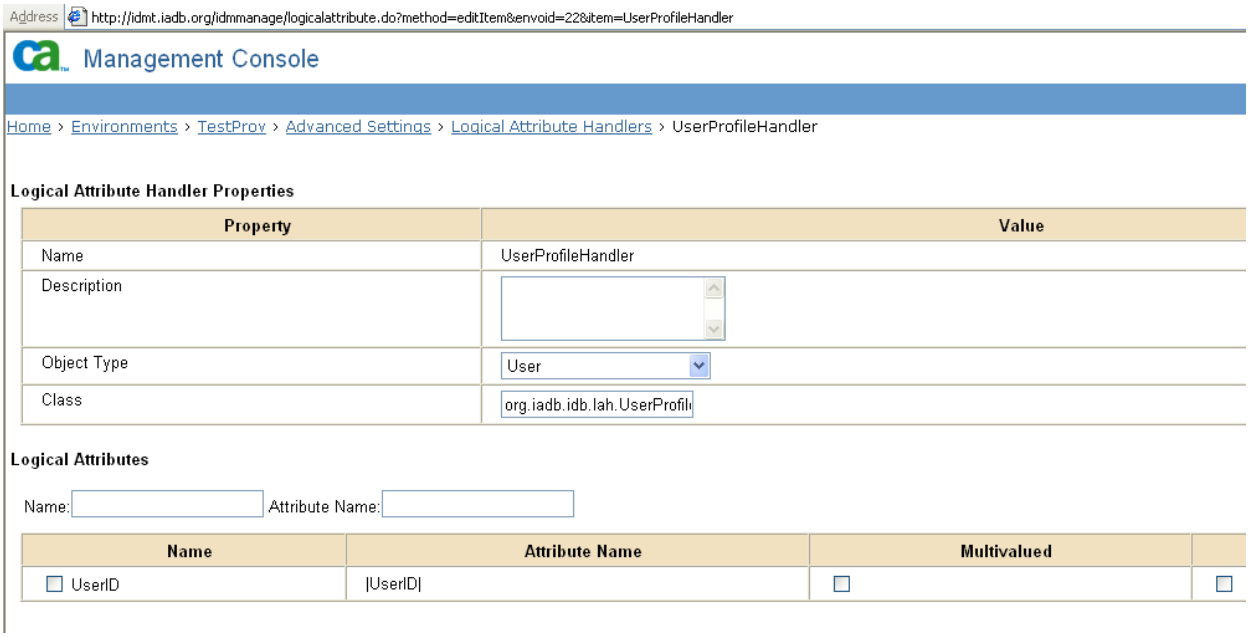
Clase de Java: org.iadb.org.lah.UserProfileAdapter

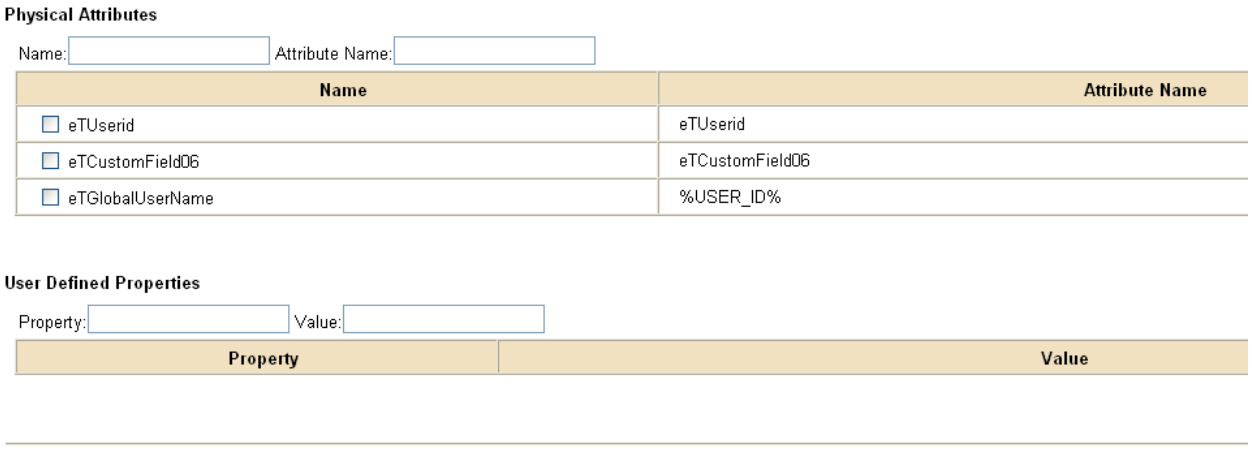
Proposito: Atributo Actualización eTUserid de eTGlobalUserName

Descripción: El ' Añadir BID usuario tarea de administración requiere eTUserid atributo oculto poblado de creación de usuarios con éxito . Este manejador atributo lógico escribe atributo eTUserid con mismo valor que eTGlobalUserName , sin tener que teclear en el formulario.

Manejador de atributo lógico se define en el

Identidad Minder Gestión Console-> IME- > Configuración avanzada > Manipuladores atributo lógico





El atributo lógico | ID de usuario | se utiliza en la pantalla de perfil de 'Agregar BID usuario tarea . El atributo eTUserid se rellena con el valor de eTGlobalUserName sobre la presentación de tareas.

21.2 ModifyUserListener

Java Clase: org.iadb.org.eventlisteners.ModifyUserListener

Propósito : Para actualizar eTCustomField06 atributo que se utiliza para detener el envío de notificaciones por correo electrónico cuando Explorar / tarea Correlate se ejecuta desde Identidad Mindereither manualmente o por un proceso programado

Descripción: Esta clase actúa como un detector de eventos para el evento ' Modificar usuario . Si el evento ' Modificar usuario se desencadena por ' Aprovisionamiento Añadir BID usuario "o" aprovisionamiento Modificar BID usuario tareas de administración , este detector de eventos reinicia el comentario notificar atributo eTCustomField06 en blanco. Notificaciones de correo electrónico se basan en la presencia del atributo eTCustomField06 . Puede ser cualquiera de los siguientes - ' Añadir usuario ', ' Transferencia de usuario ', ' Usuario Terminado ' , 'Usuario recontratados . Estos valores son establecidos por respectivos archivos por lotes ejecutable . Tan pronto como se envía una notificación, este atributo se restablece en blanco.

Para el evento de transferencia , por ejemplo , el código C # tiene un atributo comentario con estos valores

TransferUser.csc - Notepad

File Edit Format View Help

```
    static String email = "";
    static String manager = "";
    //static String phone = "";
    static String phoneext = "";
    static String status = "";
    static String olddeptid = "";
    static String oldtitle = "";
    static String managerempid = "";
    static String comment = "Transfer User";
//EAC 3-10-10 added comment field above
```

El rol de usuario transferencia sólo es necesario para la lógica de transferencia de SSIS para generar el archivo csv Transferencia corresponsal poblado de registros de transferencia.

Address http://idmt.iadb.org/idmmanage/eventlistener.do?method=editItem&envoid=22&item=ModifyUserListener

Management Console

Home › Environments › TestProv › Advanced Settings › Event Listeners › ModifyUserListener

Event Listener Properties

Property	Value
Name	ModifyUserListener
Description	Resets NOTIFY COMMENT field to blank
Class	org.iadb.idb.eventlisteners
Listener Level	ModifyUserEvent

User Defined Properties

Property: Value:

Property	Value

216

22 Mapa de atributos

22.1 Directorio corporativo y directorio de aprovisionamiento

Atributo asignaciones asocian los atributos de usuario en el almacén de Identidad Minderuser a los atributos de usuario en el directorio de aprovisionamiento. A continuación se muestra la asignación actual

Identity Minder Management Console-> con entorno > IADBProv- > Avanzado Preferencias- > Aprovisionamiento

Attribute Mappings

This section maps user attributes in the directory to user attributes in the provisioning directory.

User Attribute: %ADMIN_OF% Provisioning Attribute: %ADMIN_OF%

User Attribute	Provisioning Attribute
%ADMIN_OF%	%ADMIN_OF%
%ADMIN_ROLE_CONSTRAINT%	%ADMIN_ROLE_CONSTRAINT%
%CERTIFICATION_STATUS%	%CERTIFICATION_STATUS%
%DELEGATORS%	%DELEGATORS%
%EMAIL%	%EMAIL%
%ENABLED_STATE%	%ENABLED_STATE%
%FIRST_NAME%	%FIRST_NAME%
%FULL_NAME%	%FULL_NAME%
%IDENTITY_POLICY%	%IDENTITY_POLICY%
%LAST_CERTIFIED_DATE%	%LAST_CERTIFIED_DATE%
%LAST_NAME%	%LAST_NAME%
%PASSWORD%	%PASSWORD%
%PASSWORD_DATA%	%PASSWORD_DATA%
%USER_ID%	%USER_ID%
eTBuilding	eTBuilding
eTCity	eTCity
eTComments	eTComments
eTCompany	eTCompany

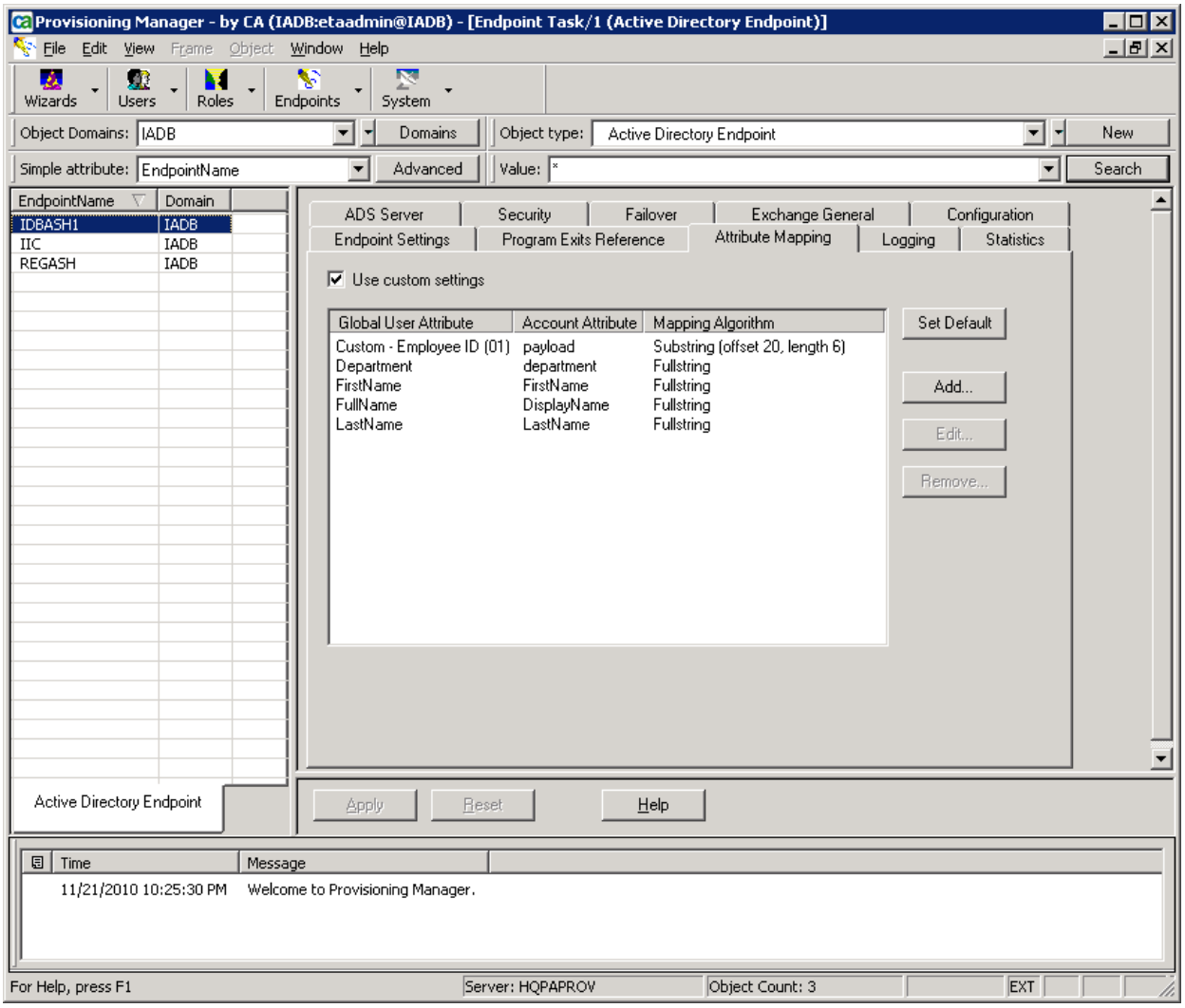
217

☐ eTCountry	eTCountry
☐ eTCustomField01	eTCustomField01
☐ eTCustomField02	eTCustomField02
☐ eTCustomField03	eTCustomField03
☐ eTCustomField04	eTCustomField04
☐ eTCustomField05	eTCustomField05
☐ eTCustomField06	eTCustomField06
☐ eTCustomField07	eTCustomField07
☐ eTCustomField08	eTCustomField08
☐ eTCustomField09	eTCustomField09
☐ eTCustomField10	eTCustomField10
☐ eTDepartment	eTDepartment
☐ eTDescription	eTDescription
☐ eTFAXNumber	eTFAXNumber
☐ eTHidefromABEXC	eTHidefromABEXC
☐ eTHomePage	eTHomePage
☐ eTHomeServerEXC	eTHomeServerEXC
☐ eTLocation	eTLocation
☐ eTMailboxStoreEXC	eTMailboxStoreEXC
☐ eTMiddleName	eTMiddleName
☐ eTMobilePhone	eTMobilePhone
☐ eTOffice	eTOffice
☐ eTPager	eTPager

☐ eTPostalCode	eTPostalCode
☐ eTStateLocalityProvince	eTStateLocalityProvince
☐ eTStreetAddress	eTStreetAddress
☐ eTTelephone	eTTelephone
☐ eTTelephoneExtension	eTTelephoneExtension
☐ eTTitle	eTTitle
☐ eTUserid	eTUserid

22.2 Directorio de aprovisionamiento y asiganacion de Active Directory

Los siguientes atributos de usuario global mapa para el usuario respectivo atributos en Active Directory



219

23 Integración de Active Directory

23.1 Integración AD, servidor abastecimiento.

Los objetos en el dominio de aprovisionamiento están protegidos en varios niveles diferentes , pero el acceso global al dominio está protegido por la seguridad de autenticación, que requiere que todos los administradores para identificarse. El servidor de aprovisionamiento se configura con el Active Directory, utilizando enchufable módulo de autenticación (PAM) .

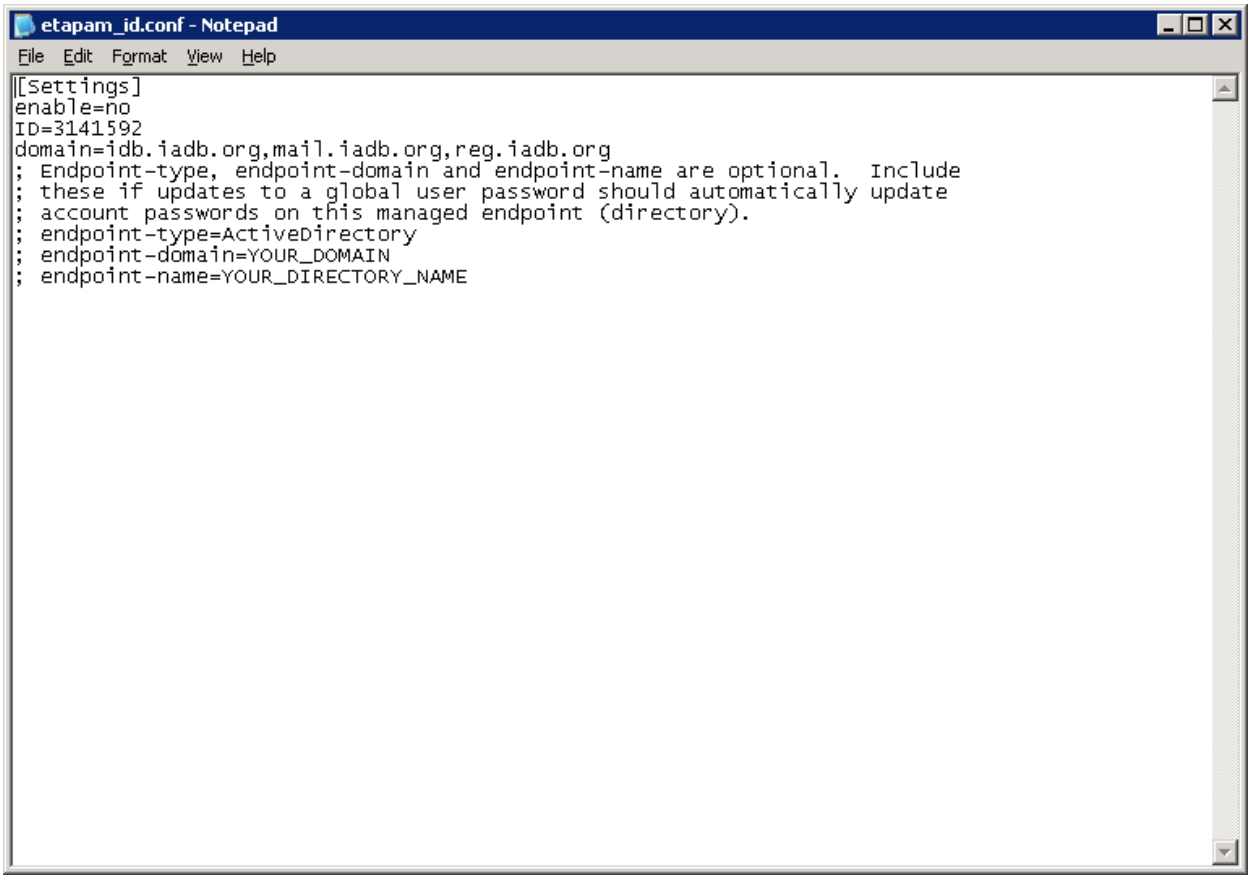
El nombre de usuario global y la contraseña que el administrador entra se autentican contra AD y autorizadas contra el directorio de aprovisionamiento .

23.1.1 Inhabilitar PAM

En orden de inhabilitar PAM, edita el archivo configuración PAM localizado en

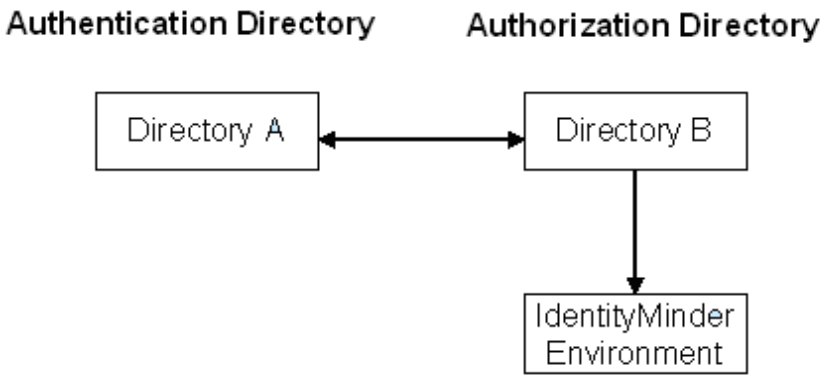
C:\ArchivosdePrograma\CA\Identity Minder\Servidordeabastecimiento\pam\etapam_id.conf

Y activar/establecer=no



23.2 Identidad de integración MinderAD

Tanto la consola y la gestión de la consola Identidad Minderuser están protegidos y se valida con las credenciales de Active Directory . La consola del usuario utiliza AD para la autenticación e identidad Minder tienda corporativa de autorización . Las tareas de administración se muestran en base al usuario rol de administrador está asignado.



23.2.1 Desactivar auntenticación AD

1. Para deshabilitar la autenticación AD para la consola de Identidad Minderuser y la consola de administración, realice los pasos a continuación

2. Ingresa en SiteMinderas con un administrador

Producción: **http://hqpasmprov/siteminder**

Prueba: **http://hqtasmpolicy/siteminder**

3. En la ficha sistemas , haga clic en dominios y haga doble clic IADBProvDomain

4. Garantizar la tienda de Identidad Minderuser es en la parte superior en el orden de búsqueda 'Directorios de usuario'

5. En la ficha Dominios , expanda IADBProvDomain

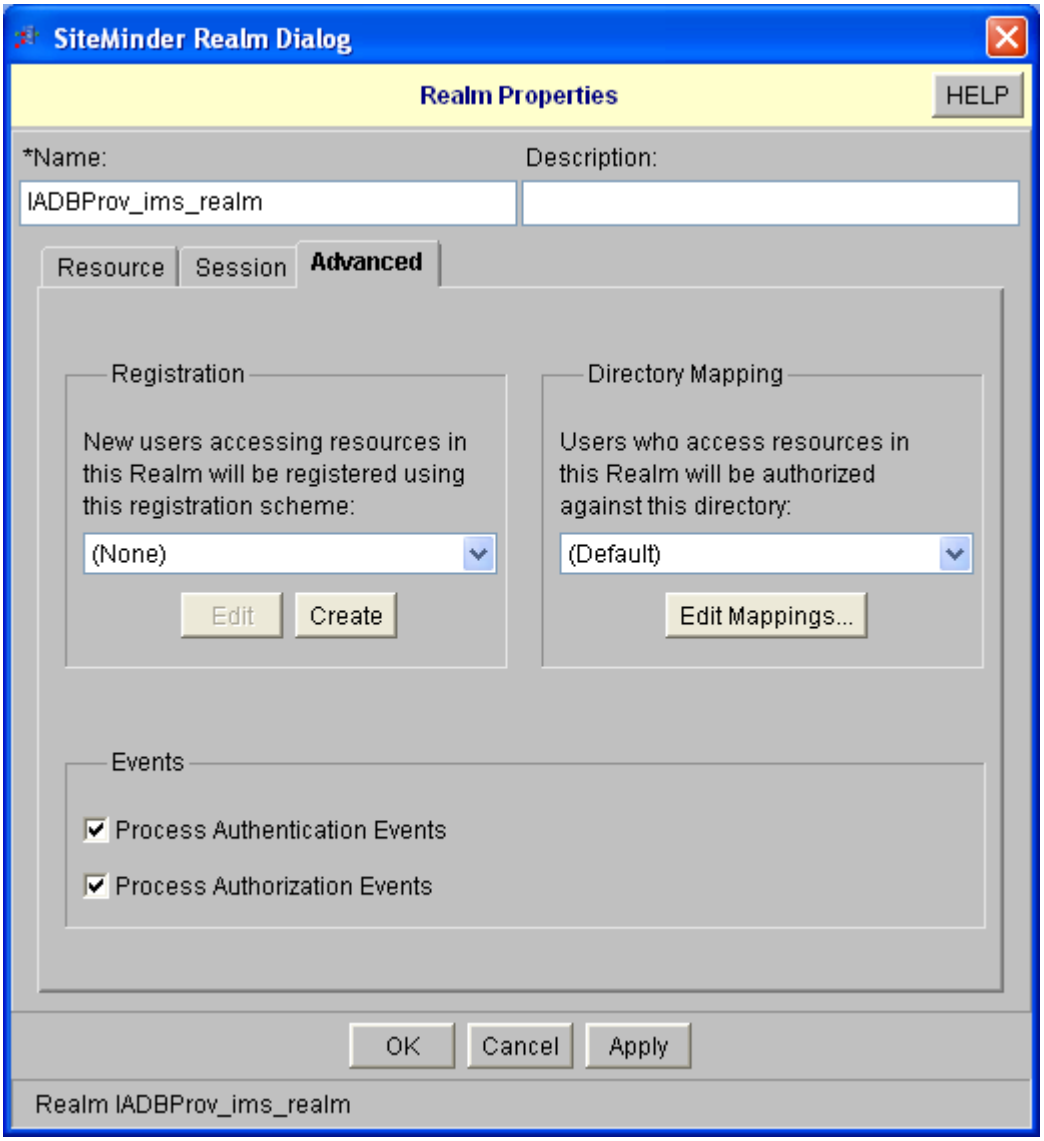
6. Haga doble clic IADBProv_ims_realm para mostrar las propiedades del dominio

7. En las propiedades del dominio , haga clic en la pestaña Avanzado

8. Seleccione Directorio de Asignaciones (por defecto)

9. Oprime OK para salir

222



23.3 MS Integración agente de cambio

IM R12.6 requiere la instalación del agente de Exchange remoto CA en los servidores de intercambio de roles buzón.

23.3.1 IADB Servidores Exchange

PROD: HQEXCHANGEO3 (cluster)

Prueba: HQEXCHANGE23 (cluster)

23.3.2 Pasos de instalación:

(Siga los pasos previstos en el documento SIS)

Grant Administrador de la organización de Exchange ; Administrador de destinatarios de Exchange ; Grupo local Administradores y también el dominio de una función de grupo \ Administradores de cuenta de AD BID \ ETA_IDB

Copie el SW Agente del intercambio 2007 de Gateway HQEXCHANGE03 (por la documentación, sólo en este servidor tenemos que el agente , [se debe instalar Remote Agent Exchange y el CAM y Servicio CAFT deben estar configurados en servidores 200x Exchange que va a utilizar como un servidor de puerta de enlace para gestionar el sitio de Exchange .] .

Instale el agente remoto de cambio como usuario [ETA_IDB] con privilegios apropiados (dominio admin / intercambio org admin)

HQEXCHANGE03 \ \ Exchange Agent CR10 \ diablillos - E2K7 - x64 -remote- agente - r12 - CR10-100219 \ RemoteAgent \ Exchange2007 \ setup.exe

Ejecutar comandos conectado como ETA_IDB :

cafthost -a HQPAPROVN.idb.iadb.org

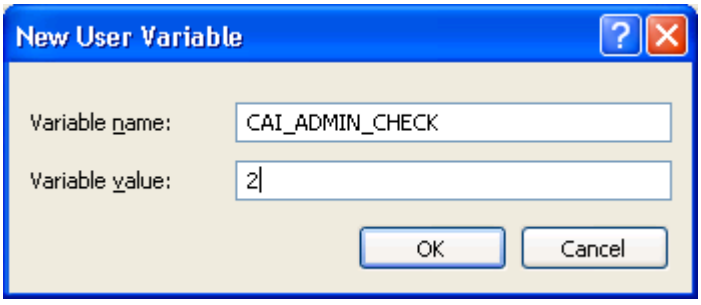
camclose

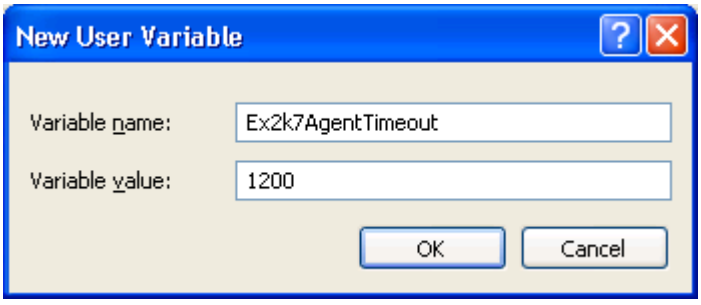
inicio Cam

Agregue la siguiente variable de entorno con un valor de "2"

CAI_Admin_check

Ex2k7AgentTimeout





Siguiendo variable de entorno se debe establecer en el aprovisionamiento de servidor para visitar el servidor de AD específico para información de la cuenta de AD antes de crear buzones de Exchange (cuando ambas acciones presentadas como parte del mismo de petición de provisión)

225


New User Variable
Variable name:
ADS_FAILOVER
Variable value:
1
OK
Cancel

226

24.1 Cuentas administrativas(ver tabla 39)

Tabla 39 – Cuentas administrativas

Cuentas administrativas	Descripción
imadminp (produccion) IMAdmin (Prueba)	Identity Minder Super user
etaadmin (Produccion) imadmintest and svc_im_prov (prueba)	Servidor super ususario de Abastecimiento
Inbound (tanto en la prueba como en la producción)	Identity Minder Corporativa usuario con rol de administrador ' Aprovisionamiento Sincronizar Administrador '
Anonymous (tanto en la producción como en las pruebas)	IM usuario que usa para accede a las areas de usuario publicas
svc_idm_userpn (produccion) svc_idm_userdn (pruebas)	IM cuenta de servicio utilizada para conectarse al servidor de base de datos SQL
Administrator (tanto en la producción como en las pruebas)	Administrador del servicio de informes
CAEmbeddedUser(Produccion) imadmintest (pruebas)	Cuenta utilizada para los componenetes de CA incrustados
imadminp (produccion) Imadmin (prueba)	IM cuenta utilizada para la administración SiteMinder
svc_eta_idb (tanto en la producción como en las pruebas)	IM cuenta de servicio utilizada para administrar la cuenta de endpoint AD BID y servicio de agente de cambio

24.2 Websphere (ver tabla 40)

Tabla 40 – Websphere

Nombre del campo	Descripción	Valor
WebSpherecarpeta de instalación	La ubicación de la aplicación directorio de inicio del servidor .	D:Program Files\IBM\WebSphere\AppServer
Nombre del servidor	El nombre del sistema en	Prod: hqpaidmn

	que el servidor de aplicaciones se está ejecutando.	Test: hqdaidmn
Nombre de perfil	El nombre del perfil que que desee utilizar para Identity Manager.	AppSrv01
Nombre de celula	El nombre de la celda en la que el servidor de aplicaciones es ubicado.	Prod: HQPAIDMNode01Cell Test: HQDAIDMNode01Cell
Nombre de nodo	El nombre del nodo en el cual el servidor de aplicaciones es ubicado.	Prod: HQPAIDMNode01 Test: HQDAIDMNode01
Puerto	El puerto del servidor de aplicaciones está escuchando.	9080
URL	La URL del servidor de aplicaciones	Prod: http://hqpaidmn.idb.iadb.org:9080 Test: http://hqdaidmn.idb.iadb.org:9080

24.3 Directorio de abastecimiento(ver tabla 41)

Tabla 41 – Directorio de abastecimiento

Nombre del campo	Valor	Value
Hospedaje	El nombre de host del sistema remoto Directorio de aprovisionamiento.	Prod: HQPAPROVN Test: HQDAPROVN
Puerto	El número de puerto de un sistema remoto Directorio de aprovisionamiento.	20391
DSA Contraseña	El aprovisionamiento remoto Contraseña de usuario de directorio.	-
Nombre de dominio	El nombre de dominio para el Directorio de aprovisionamiento.	IADB
Java componenetes contraseá	Contraseña para el servidor Java Connector fijado en el momento de la instalación	-

228

24.4 Base de datos(ver tabla 42)

Tabla 42 – Base de datos

Nombre del campo	Descripción	Valor
Tipo de base de datos	El tipo de base de datos (vendor / version) del base de datos creada para la tarea persistencia, flujo de trabajo, auditoría, informes y almacén de objetos .	Microsoft SQL Server 2008
Nombre de hospedaje	El nombre de host del sistema donde se encuentra la base de datos.	Prod: IDBPRDA1\IDBPRDA1INST1 Test: IDBTRDA1\IDBTRDA1INST1
Numero de puerto	El número de puerto del base de datos.	Prod: 1518 Test: 2974
SID/nombre de base de datos	El identificador de base de datos.	Prod: IDM_DBPRODN & IDM_REPPRODN Test: IDM_DBDEVN & IDM_REPDEVN
Nombre de usuario	El nombre de usuario de base de datos Acceso con derechos administrativos.	Prod: svc_idm_prep Test: svc_idm_userdn
Contraseña	La contraseña para el usuario cuenta con administrativa los derechos .	Consultar hoja maestra contraseña

24.5 Politicas de servicio(ver tabla 43)

Tabla 43 – Politicas de servicio

Nombre de campo	Descripción	Valor
Nombre del hospedaje políticas de servicio	El nombre de host del SiteMinderPolicy Server.	Prod: hqpasmprovn/ Test: hqtasmpolicy
SiteMinder Nombre de administrador	El nombre de usuario administrador el servidor SiteMinderPolicy .	Prod: imadminp Test: imadmin

229

SiteMinder Contraseña de administrador	Contraseña de administrador de usuarios de la SiteMinder políticas de servicio	-

230

25 Notificaciones de los eventos que procesa el provisioning process.

25.1 Email plantillas

Email notificaciones estan configuradas por las siguientes tareas de administrador..

- Add IADB User
- Transfer IADB User
- Terminate IADB User
- Rehire IADB User
- Provisioning Add IADB User
- Provisioning Modify IADB User

Cuando cualquiera de estas tareas completa , Identity Minder Envía una notificación de correo electrónico. El contenido del correo electrónico se define en las plantillas de correo electrónico en la siguiente ubicación

Está es la ruta del servidor hqpaidmn(Application Server) donde se encruentran los scripts con la lógica que siguen las notificaciones de e-mail de los eventos procesados por el provisioning process

C:\IBM\WebSphere\AppServer\profiles\IADB_IM1\installedApps\HQPAIDMNode02Cell\IdentityMinder.ear\custom\emailTemplates\default\completed

Las reglas necesarioas para configurar las notificaciones son:

Oficinas locales en los paises:

1) CAR

Transfer

Para: **CARTechSup@iadb.org**; **sqainfosec@iadb.org**; **EMAILGROUP@iadb.org**; **ITECOMPLIANCE@iadb.org**

Cc:

Nuevo usuario

Para: **CARTechSup@iadb.org**; **SQAINFOSEC@iadb.org**;**EMAILGROUP@iadb.org**

Terminación

para: **CARTechSup@iadb.org**; **sqainfosec@iadb.org**; **EMAILGROUP@iadb.org**; **ITECOMPLIANCE@iadb.org**

recontratación

Para: **CARTechSup@iadb.org**; **SQAINFOSEC@iadb.org**;**EMAILGROUP@iadb.org**

2) CBA

Transferencia

Para: **CBATechSup@iadb.org**; **sqainfosec@iadb.org**; **EMAILGROUP@iadb.org**; **ITECOMPLIANCE@iadb.org**

CC:

Nuevo Usuario

Para: **CBATechSup@iadb.org**; **SQAINFOSEC@iadb.org** ;**EMAILGROUP@iadb.org**

Cc:

Terminación

Para: **CBATechSup@iadb.org**; **sqainfosec@iadb.org**; **EMAILGROUP@iadb.org**; **ITECOMPLIANCE@iadb.org**

Recontratación

Para: **CBATechSup@iadb.org**; **SQAINFOSEC@iadb.org** **;EMAILGROUP@iadb.org**

Resto de las ciudades:

CBH, CBL, CBO, CBR, CCH,CCO, CDR, CCR, CEC, CES, CFR, CGU, CGY, CHA, CHO, CJA, CJP, CME, CNI, CPE, CPN, CPR, CSU, CTT, CUR, CVE

Sede:

Transferir

Para: **sgainfosec@iadb.org**; **Helpdesk@iadb.org;EMAILGROUP@iadb.org**; **ITECOMPLIANCE@iadb.org**

CC:

Nuevo Usuario

Para: **SQAINFOSEC@iadb.org** ; **Helpdesk@iadb.org**; **EMAILGROUP@iadb.org**

Cc:

Terminación

Para: **sgainfosec@iadb.org**; **Helpdesk@iadb.org**; **EMAILGROUP@iadb.org**; **ITECOMPLIANCE@iadb.org**

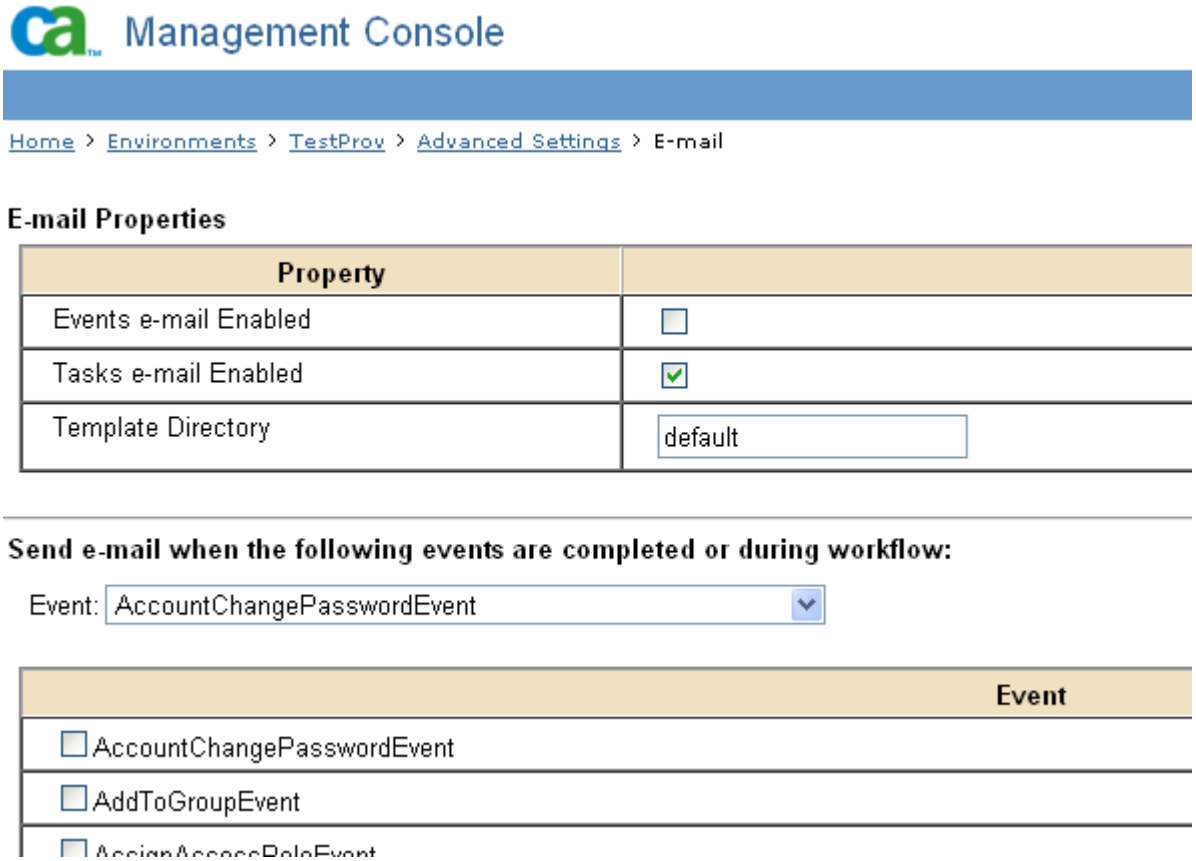
Recontratación

Para: **SQAINFOSEC@iadb.org** ; **Helpdesk@iadb.org**; **EMAILGROUP@iadb.org**

25.2 Configuración

Navega a la Identidad Minder Gestión Console-> con entorno > IME- > Preferencias avamzadas- > Email

Casilla de verificación Seleccionar para ' Tareas de correo electrónico habilitada ' para habilitar las notificaciones de tareas



Añadir last areas de la lista de notificaciones.

234

Send e-mail when the following tasks are completed or during workflow:

Select a task by performing a search and selecting from the results:

Admin Task Name: EQUALS

Search Results:

Name

Task
Add IADB User
Forgotten Password
Provisioning Add IADB User
Provisioning Modify IADB User
Rehire IADB User
Terminate IADB User
Transfer IADB User

26 Solución de problemas del entorno de Identity Minder

26.1 Verificar estado de IME

Identidad Minder incluye una página de estado que se puede utilizar para verificar lo siguiente:

- El directorio de identidad Minder está cargado correctamente
- Identidad Minder se puede conectar a la tienda de usuario
- Las cargas Identidad Minderenvironment correctamente

Para acceder a la página de estado , escriba el siguiente URL en un navegador:

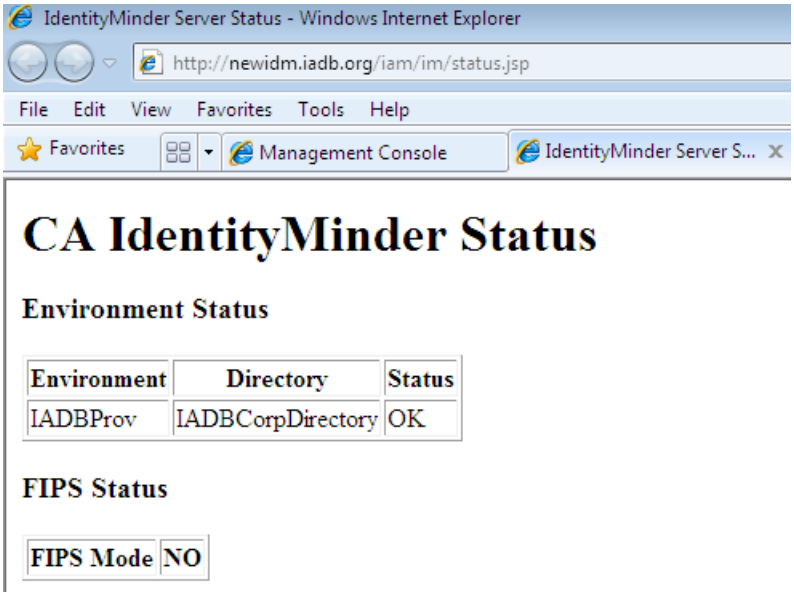
Producción :

http://newidm.iadb.org/iam/im/status.jsp

Prueba:

http://idmt.iadb.org/iam/im/status.jsp

236



26.2 Ver tareas enviadas

CA Identity Minder incluye tarea 'Ver tareas enviadas" para mostrar el estado de todos los eventos y tareas en un entorno de Identity minder. Los administradores utilizan esta tarea en el usuario de la consola.

Ver Tareas enviadas proporciona los siguientes tipos de información:

• La lista de eventos y tareas que se producen en el medio ambiente

• La lista de atributos asociados a un evento

• eventos exitosos y fallidos

• Eventos que están en un estado pendiente o estancado

• Eventos rechazadas, incluyendo el motivo del rechazo

• estado de sincronización de cuentas

• Estado de la sincronización de políticas de identidad

• La información de aprovisionamiento (cuando aprovisionamiento está habilitado)

26.2.1 Buscar Atributos de Visualización Enviado Tareas

Para revisar las tareas que se han presentado para su procesamiento, puede utilizar la función de búsqueda en Tareas Ver Enviado. Usted puede buscar tareas en función de los siguientes criterios:

Iniciado por

Identifica el nombre del usuario que ha iniciado una tarea como los criterios de búsqueda. Búsquedas se basan en el nombre de usuario. Para asegurarse de que ha introducido un nombre de usuario válido, utilice el botón Validar.

Tareas de aprobación Realizado Por

Identifica el nombre del aprobador tarea como los criterios de búsqueda. Búsquedas se basan en el nombre de usuario. Para asegurarse de que ha introducido un nombre de usuario válido, utilice el botón Validar.

Nota: Si selecciona tareas de aprobación realizado por criterios para filtrar las tareas, los criterios en Mostrar tareas de aprobación también está habilitada por defecto.

Nombre de la tarea

Identifica el nombre de la tarea como criterio de búsqueda. Puede refinar la búsqueda especificando condiciones tales como iguales, contiene, empieza por o termina con el valor de la Dónde campo Nombre de tarea. Por ejemplo, puede especificar los criterios de búsqueda "nombre de la tarea es igual Crear usuario" mediante la selección de la condición de iguales, y entrar en Crear usuario en el campo de texto.

Estado de Tareas

238

Identifica estado de la tarea como criterio de búsqueda. Puede seleccionar el estado de la tarea al permitir Dónde estado de la tarea es igual, y la selección de la condición. Puede refinar más la búsqueda en base a las siguientes condiciones:

- Completado
- En curso
- Falló
- Rechazado
- Parcialmente completada
- Cancelado
- Programado

Nota: Consulte Estado de tarea Descripción para más información.

Prioridad de tareas

Identifica la prioridad tarea como los criterios de búsqueda. Puede seleccionar la prioridad de la tarea al permitir Dónde es igual prioridad de la tarea, y la selección de la condición. Puede refinar más la búsqueda en base a las siguientes condiciones:

Bajo

Especifica que usted puede buscar para las tareas que tienen una baja prioridad.

Medio

Especifica que usted puede buscar para las tareas que tienen una prioridad media.

Alto

Especifica que usted puede buscar para las tareas que tienen una alta prioridad.

Realizado En

Identifica las tareas que se realizan en la instancia seleccionada del objeto. Si no selecciona una instancia del objeto, se mostrarán las tareas que se realizaron en todas las instancias de ese objeto.

Nota: Este campo sólo aparece cuando Configurar realiza en campo se rellena en la pantalla de Tareas Configurar Enviado. Utilice esta pantalla para configurar la ficha Tareas Enviado. Consulte la ayuda en línea para que la pantalla para obtener más información.

Intervalo de fechas

Identifica las fechas entre las que desea buscar tareas presentadas. Debe proporcionar la fechas Desde y Hasta.

Mostrar tareas no enviados

Identifica las tareas en el Estado auditado. Identifica las tareas que han iniciado tareas o tareas que no han sido presentados. Todas estas tareas serán auditados y se muestran si se selecciona esta ficha.

Mostrar tareas de aprobación

Identifica las tareas que tienen que ser aprobados como parte de un flujo de trabajo.

Buscar archivo de tareas presentadas

Identifica las tareas presentadas que han sido archivados.

26.3 Registro de aplicación de servicios

Muestra información sobre todos los componentes de una instalación de identidad Minder , y proporciona detalles acerca de todas las operaciones en Identidad Minder . Por ejemplo , los errores y las advertencias de Notificaciones .

Registro Websphere se escribe

:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\SystemOut.log

26.4 Archivo de registro del servidor de directorios corporativos.

Contiene información sobre la actividad que se produce en el directorio de usuario situado en HQPACORPN

(Production)/ HQDACORPN (Prueba)

D:\Program Files\CA\Directory\dxserver\logs

26.5 Registo de aprovisionamiento de servidor

(Nota : Este registro es el mismo que las versiones anteriores)

Localización de los registros: los registros del servidor de aprovisionamiento se escriben en archivos de texto en el D: \ Archivos de programa (x86) \ CA Identity Manager \ Provisioning Server \ logs y se nombran en consecuencia:

Los componentes de aprovisionamiento (Provisioning Server, servidores de conector, Provisioning Manager) se pueden configurar para registrar información sobre todas las transacciones

que se procesan. Puede utilizar esta información para predecir e identificar las fuentes de la seguridad del sistema o problemas. Por ejemplo, si los mensajes de advertencia en los archivos de registro muestran que algunas cuentas en un punto final no se podrían explorar, puede utilizar la información registrada para investigar esas cuentas y determinar por qué no fueron exploradas. Utilice un editor de texto para ver y editar archivos de registro de aprovisionamiento.

Los registros de eventos del servidor seguimiento de los mensajes generados por el servidor de aprovisionamiento. Usted puede registrar mensajes a varios destinos opcionales, incluyendo CA Audit.

Los componentes de aprovisionamiento proporcionan otros tipos de registro para diagnosticar problemas específicos. Aparte del registro de seguimiento del servidor de aprovisionamiento, estos registros son por lo general no permitieron a menos que usted los necesita para rastrear un evento en particular. Incluyen los registros del servidor de aprovisionamiento, registros slapd y los registros de C ++ Connector Server. También puede diagnosticar los problemas que se producen cuando se comunica con el servidor de aprovisionamiento habilitando el registro Gestor de aprovisionamiento.

Los mensajes de todos los registros se escriben en archivos de texto en el directorio pshome \ Logs y se nombran en consecuencia:

Provisioning Server Registro de eventos - etayyyymmdd.log

Provisioning Server registro de seguimiento - etatransyyyymmdd-hhmm.log

Provisioning Server IMS Notificación Log - etanotifyyyyymmdd-hhmm.log

Provisioning Server SLAPD Log - im_ps.log

Provisioning Manager Log - etaclientyyyymmdd.log

C ++ Conector Servidor Punto Log - sayyyymmdd.log

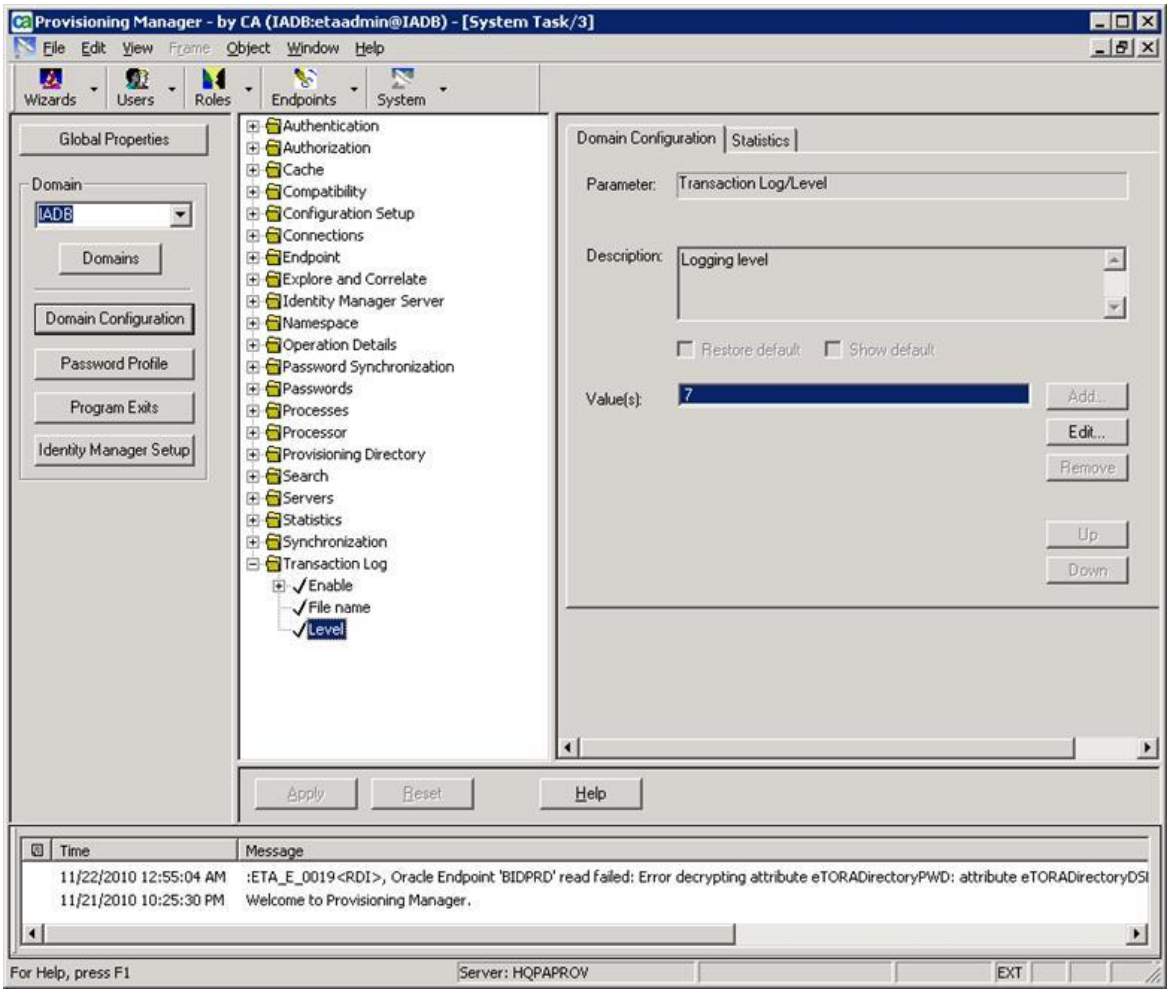
C ++ conector Servidor de registro de seguimiento - satransyyyymmdd-hhmm.log

C ++ Conector Servidor SLAPD Log - im_ccs.log

Para configurar el registro de depuración, que el nivel de seguimiento 7 de la siguiente manera

Inicia sesión para Provisioning Manager-> Sistemas> Dominio Configuración-> Transacción Log-> Activar-> Establecer SÍ

Set Activar-> Nivel-> 7 (cambió a 3 más adelante)



26.5.1 SLAPD and C++ y registros del servidor del conector C++

En Windows, puede habilitar SLAPD registro para tareas de depuración avanzadas tales como

el manejo de paquetes de protocolo LDAP y buscar-filtro de procesamiento. Puede configurar el nivel de registro en el registro de Windows mediante la asignación de un valor a la clave DebugLevel.

Hay dos claves de registro, cada control de la tala de uno de los servicios:

HKEY_LOCAL_MACHINE \ SOFTWARE \ ComputerAssociates \ slapd \ im_ps \ CurrentVersion \ DebugLevel

Los im_ps Registro controles clave madereras para im_ps.exe, dirigido por el servicio del servidor de aprovisionamiento.

HKEY_LOCAL_MACHINE \ SOFTWARE \ ComputerAssociates \ slapd \ im_ccs \ CurrentVersion \ DebugLevel

Los im_ccs Registro controles clave madereras para im_ccs.exe, dirigido por el servicio Conector Server.

Importante! El método preferido para habilitar el registro SLAPD es estableciendo el parámetro nivel de registro en im_ps.conf o im_ccs.conf, tanto para Windows y Solaris. Cada archivo contiene instrucciones de configuración.

La clave de registro DebugLevel o parámetro archivo de configuración del nivel de registro especifica la cantidad de información que el servidor escribe en su archivo de registro, que es uno de los siguientes, dependiendo de su tipo de servicio slapd:

Pshome \ Logs \ im_ps.log

Pshome \ Logs \ im_ccs.log

Nota: A "TLS: no puede aceptar" mensaje de error puede aparecer en el archivo im_ps.log cuando se ejecuta en modo FIPS debido a un problema de inicialización de bajo nivel que desaparece después de la primera conexión de un cliente. Desde clientes reintento conexiones, puede ignorar este mensaje.

Usted puede seleccionar un nivel de depuración para que coincida con el tipo de depuración que desea realizar. Los niveles de depuración se enumeran en la siguiente tabla:

Tabla 45 –

Value	Debug Information
1	Trace function calls
2	Debug packet handling
4	Heavy trace debugging
8	Connection management
16	Print out packets sent and received
32	Search filter processing
64	Configuration file processing (DEFAULT SETTING)
128	Access control list processing
256	Stats log connections/operations/results
512	Stats log entries sent
1024	Print communication with shell back-ends
2048	Entry parsing
65535	All tracing

26.6 Registros de directorio de aprovisionamiento

Contiene información sobre la actividad que se produce en el directorio de usuario situado en HQPAPROVN (Producción) / HQDAPROVN (Prueba) y están inscritos en el siguiente ruta

245

D:\Program Files (x86)\CA\Directory\dxserver\logs

(Refer CA product documentation for more details)

26.7 Archivo de registro de servidor politicas de SiteMinder

Muestra la siguiente información :

• Problemas de conexión SiteMinder

• Cuestiones SiteMinderauthentication

• Información sobre IdentityMindermanaged objetos en la tienda SiteMinderpolicy

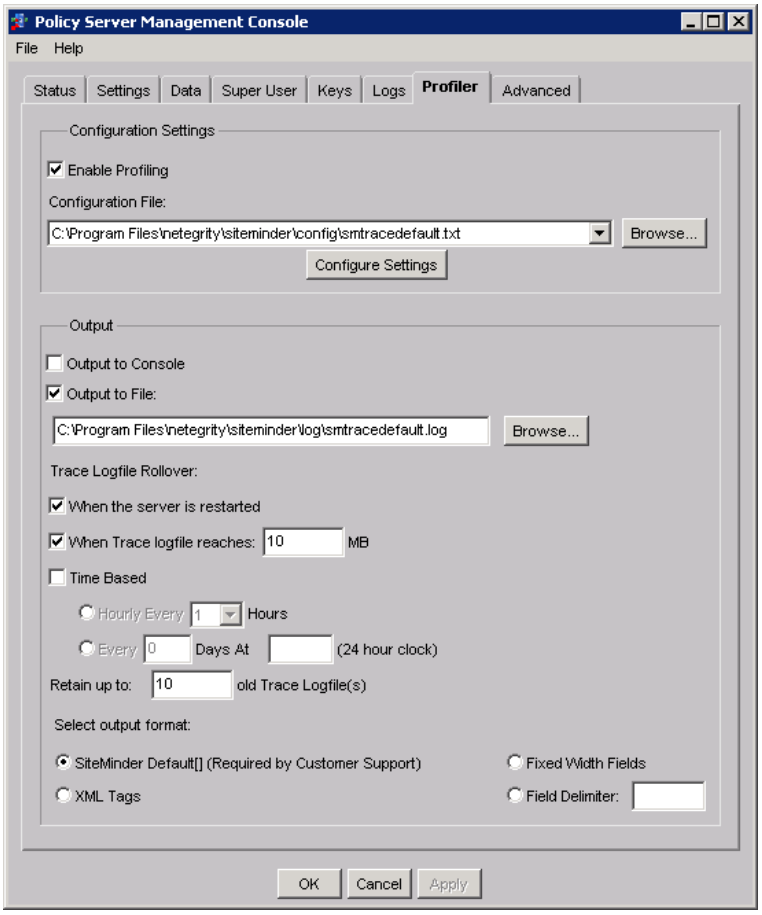
• evaluación de las políticas de contraseña

Registro del servidor política se escribe en smps.log / smaccess.log en la siguiente ubicación : hqpasmidm02 o hqpasmidm02 (en producción) y hqtasmidm01 (en prueba)

Perfilador servidor de políticas puede ser configurado para escribir mensajes detallados para smtracedefault.log y se puede configurar de la siguiente

Inicio-> Todos los programas- > Siteminder- > SiteMinderPolicy Server Management Console

Inicio-> Todos los programas- > CA- > consola de administración SiteMinder



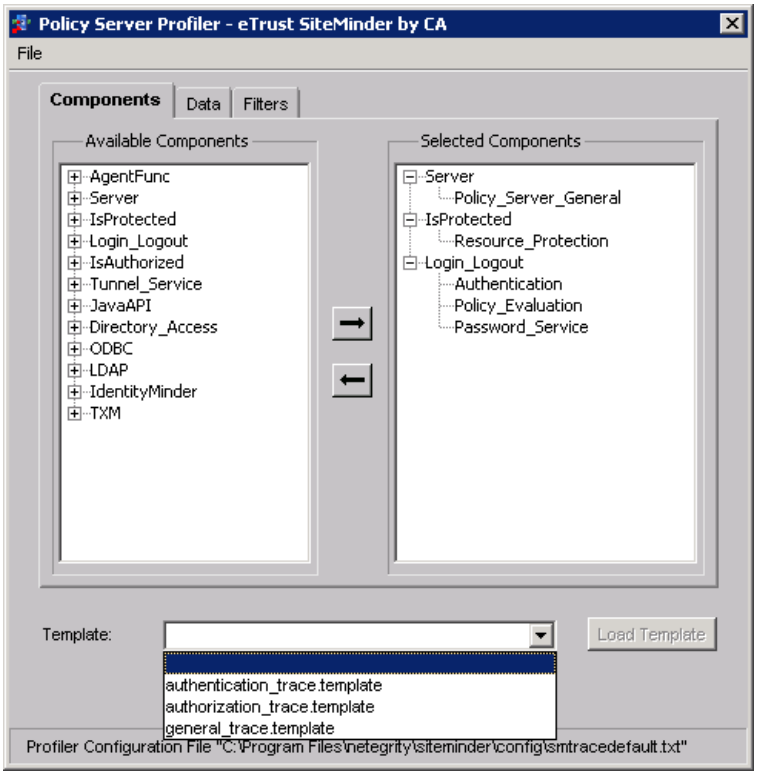
Haga clic en Configurar opciones , seleccionar componentes individuales para registrar mensajes o seleccione una plantilla y pulse Aceptar

Actualmente las plantillas en uso son :

Authentication_trace.template

Authorization_trace.template

General_trace.template



Archivos de registro de ubicación

Los registros Política SiteMinder Server se escriben en la ruta del directorio

Prueba – HQTASMIDM01 - C:\Program Files (x86)\CA\siteminder\log

PRODUCCIÓN – HQPASMIDM01 & HQPASMIDM02 - C:\CA\siteminder\log

- SMPS.log
- Smtracedefault.log
- Smaccess.log

26.8 Archivos del registro de agentes Web

Los agentes Web escriben información para los siguientes dos registros:

■ Registro de errores en archivos contiene errores de programa y de nivel operativo , por

ejemplo , el agente Web no poder comunicarse con el Servidor de directivas .

Actualmente escrito a C: \ Temp \ smagent.log en servidores : hqpniweb07 y hqpniweb08 (en producción) y hqdni06 (en prueba)

■ registro de seguimiento de archivos contiene advertencias e informaciones mensajes, como los mensajes de seguimiento y el flujo de mensajes de estado . También incluye datos como detalles del encabezado y variables de galletas.

Actualmente escrito a C: \ Temp \ smtrace.log en servidores : hqpniweb07 y hqpniweb08 (en producción) y hqdni06 (en prueba)

249

27 Performance Tuning

27.1 Configurar el agente de Identity Minder

Identidad Minder utiliza un sistema incorporado en agente de Identidad Minder para comunicarse con la Política de SiteMinder

Server. Para ajustar el rendimiento , configure los siguientes ajustes de conexión para el agente Identidad Minder .

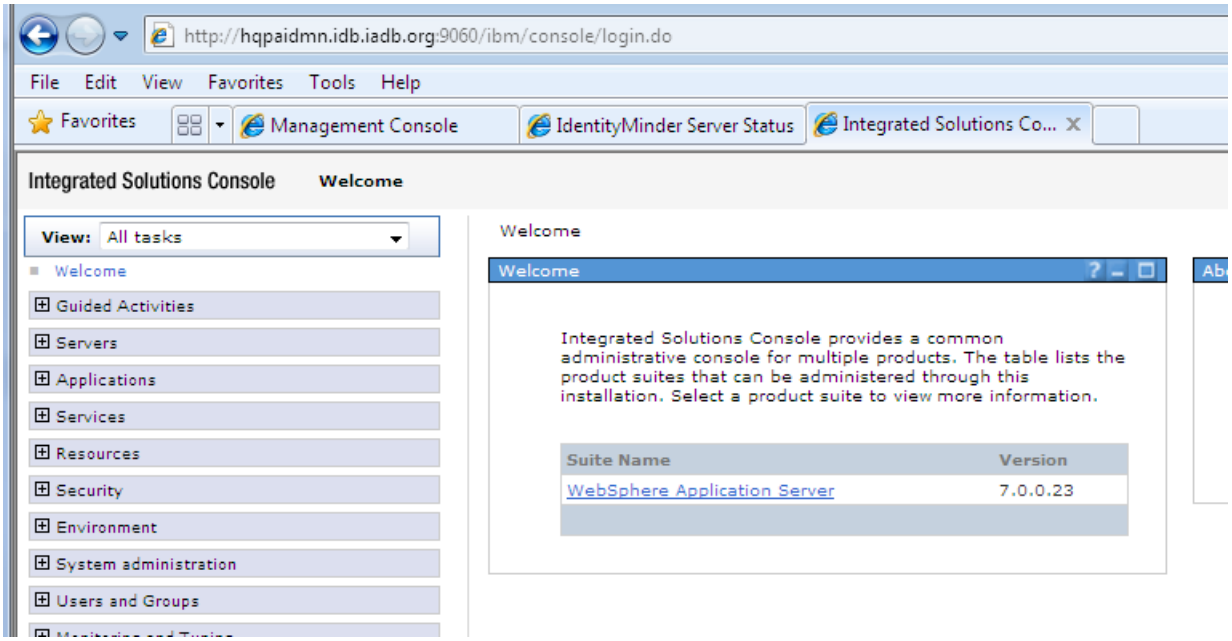
1. Realice uno de los siguientes pasos:

■ Edite el adaptador de recursos en el descriptor de conector policyserver_rar en la consola del servidor de aplicaciones.

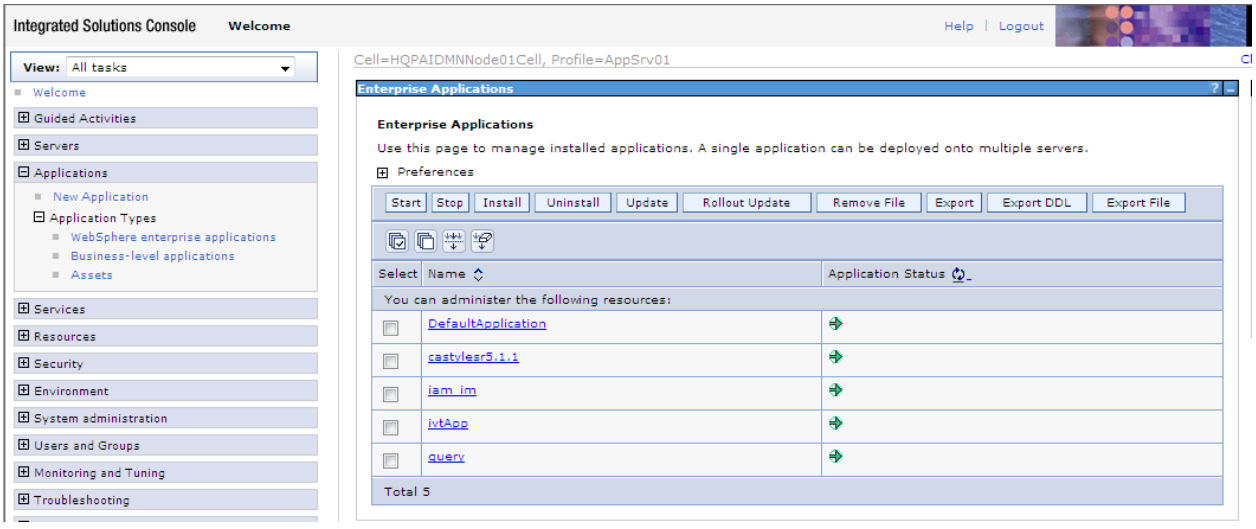
Inicia sesión para consola de administración de IBM

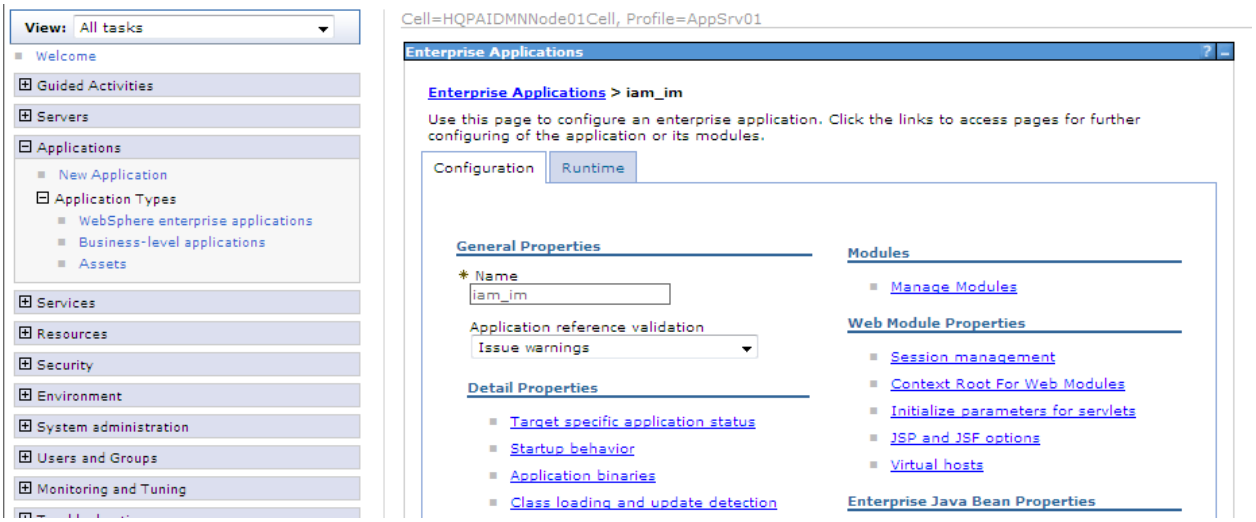
http://hqpaidmn.idb.iadb.org:9060/ibm/console (producción)

http://hqdaidmn.idb.iadb.org:9060/ibm/console (prueba)

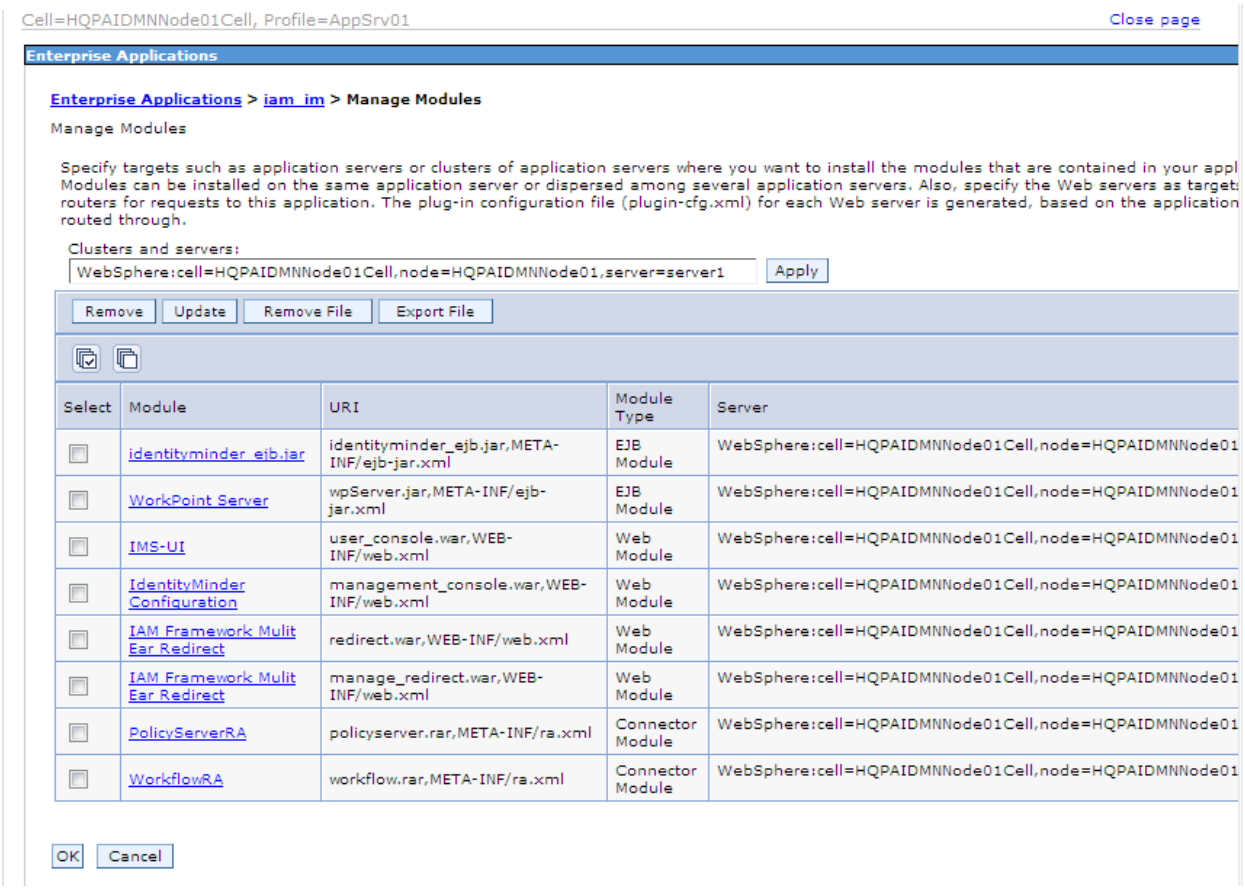


Vaya a Aplicaciones- > Aplicaciones de empresa y seleccione IdentityMinder

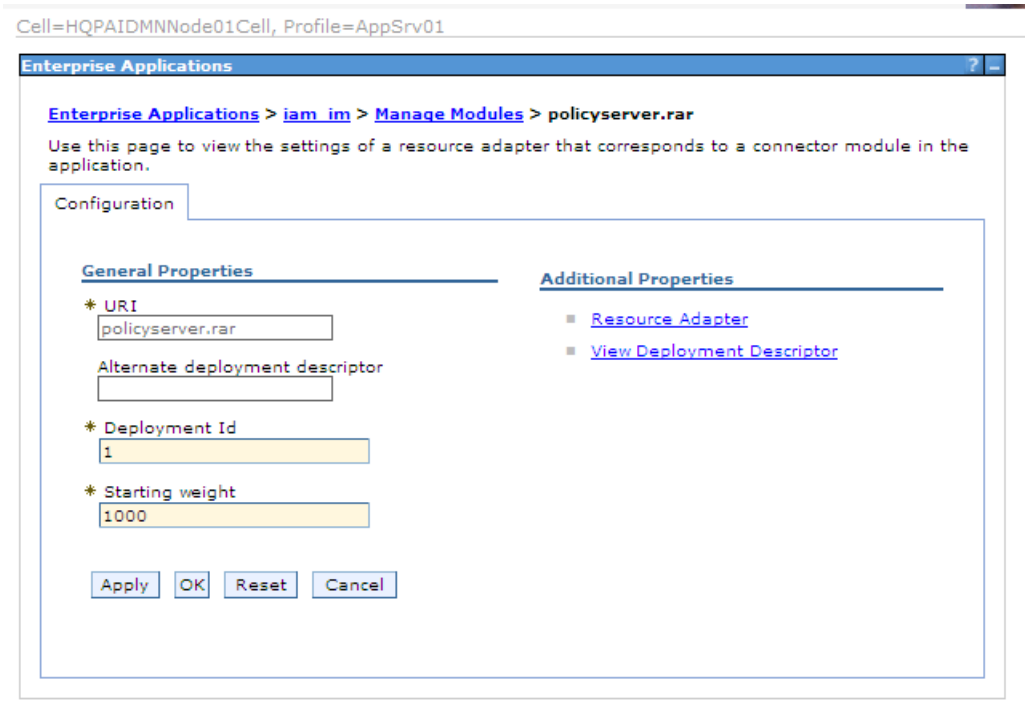




Seleccione gestionar módulos

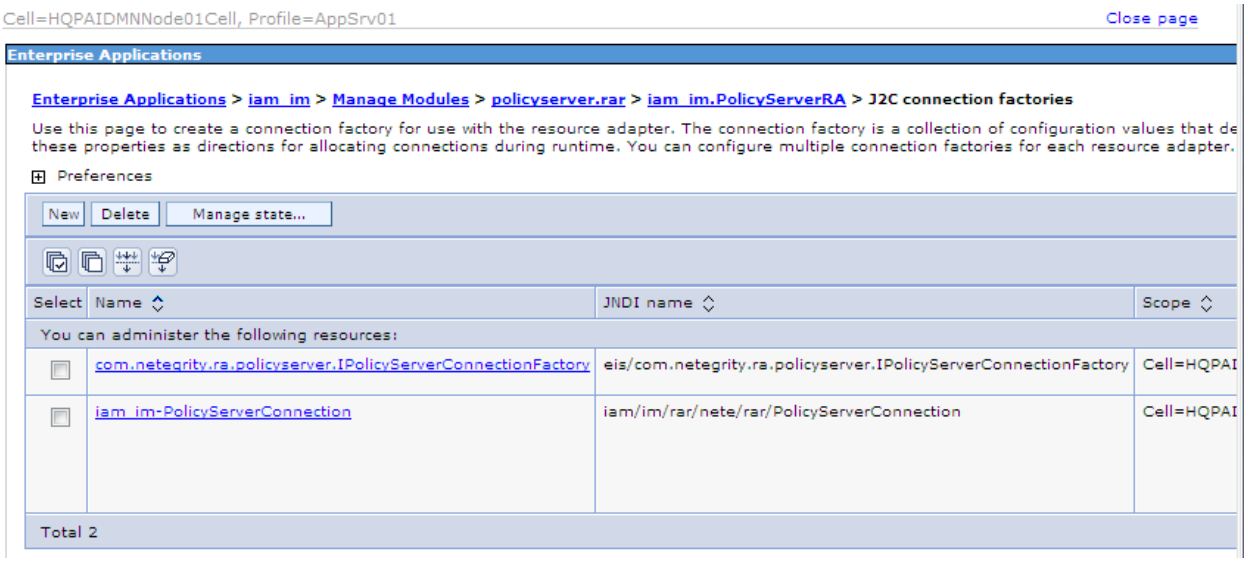


Seleccione PolicyServerRA

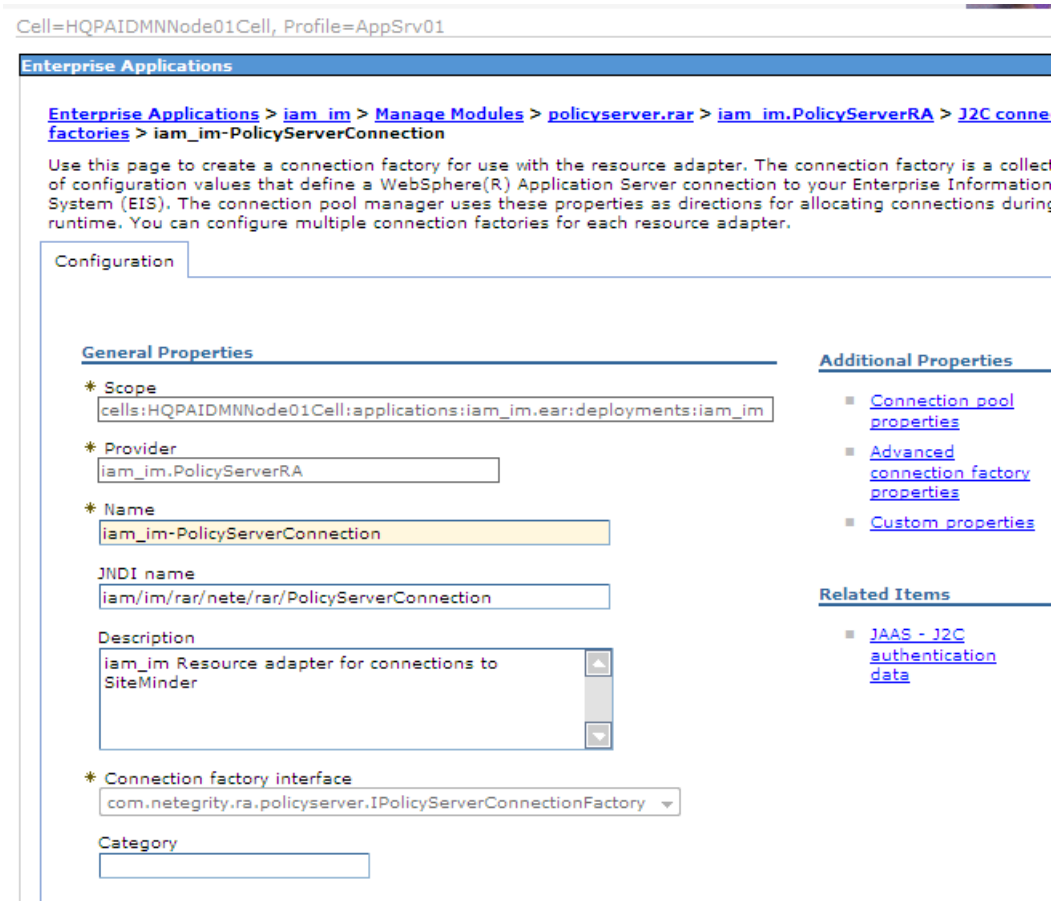


Seleccione Resource Adapter

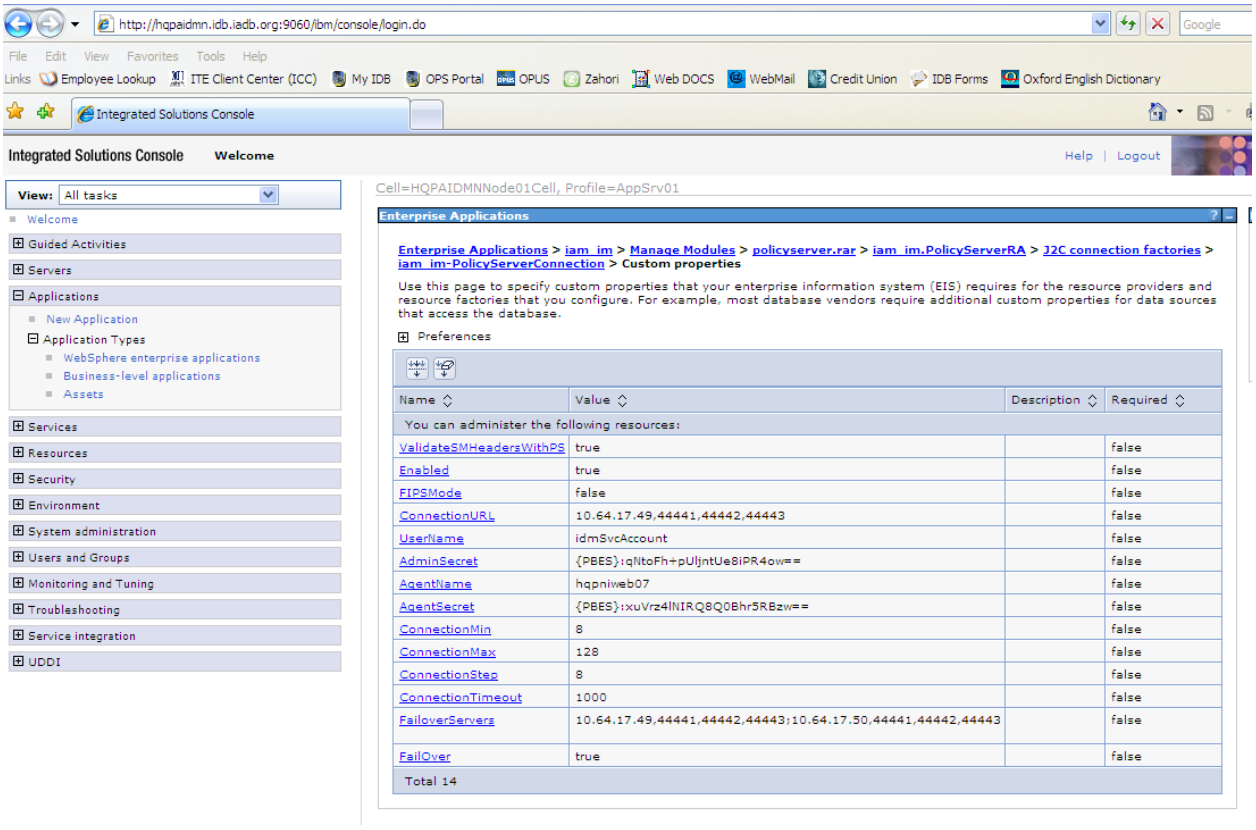
Select J2C fábricas de conexiones



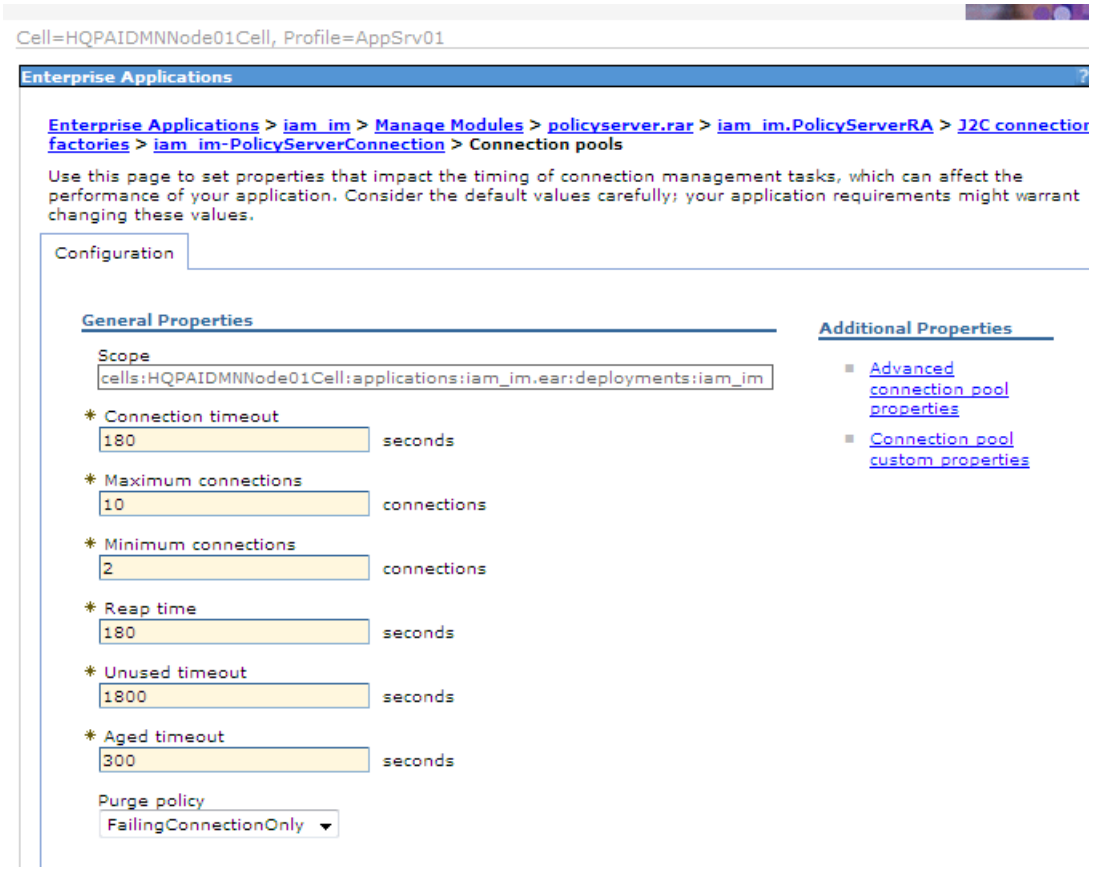
Seleccione Politicas de servidor de conección



Seleccione las propiedades personalizadas para ver parámetros Intergration SM

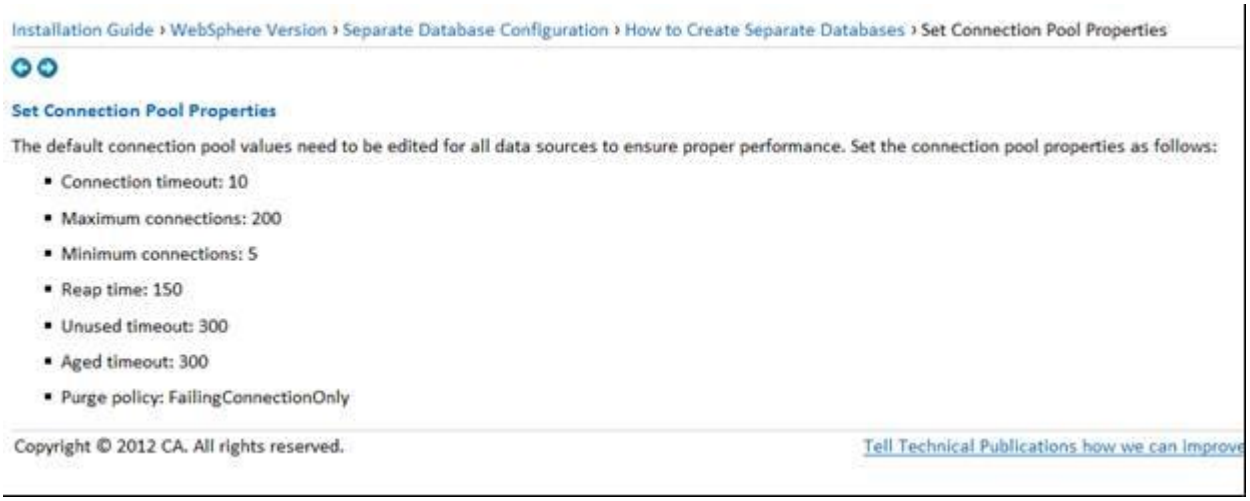


Volver a la pantalla anterior y seleccione Connection Pools



2. Configure los ajustes de la siguiente manera :

CA recomienda valores son los siguientes y éstas deben ajustarse a la habitación entorno cliente



A continuación se presentan las definiciones de los parámetros

ConnectionMax

Establece el número máximo de conexiones con el servidor de políticas, por ejemplo, 20.

ConnectionMin

Establece el número mínimo de conexiones con el servidor de políticas, por ejemplo, 2.

ConnectionStep

Establece el número de conexiones adicionales para abrir cuando todas las conexiones de agentes están en uso.

El tiempo de conexión expiro

Especifica la cantidad de tiempo que la conexión debe esperar antes de tiempo de espera.

Tiempo de espera de Ancianos

Especifica el intervalo en segundos antes de que se descarta una conexión física.

Por ejemplo, si el valor de Tiempo de espera superado se establece en 1200, y el valor del tiempo Reap no es 0, cualquier conexión física que se mantiene en la existencia por 1200 segundos (20 minutos) se descarta de la piscina.

Política de Purga

Especifica cómo purgar conexiones cuando se detecta una conexión rancio o error de conexión fatal.

Si se establece la política de purga para este objeto de origen de datos para FailingConnectionOnly, sólo la conexión que provocó el StaleConnectionException está cerrada.

3. Reinicie el servidor de aplicaciones.

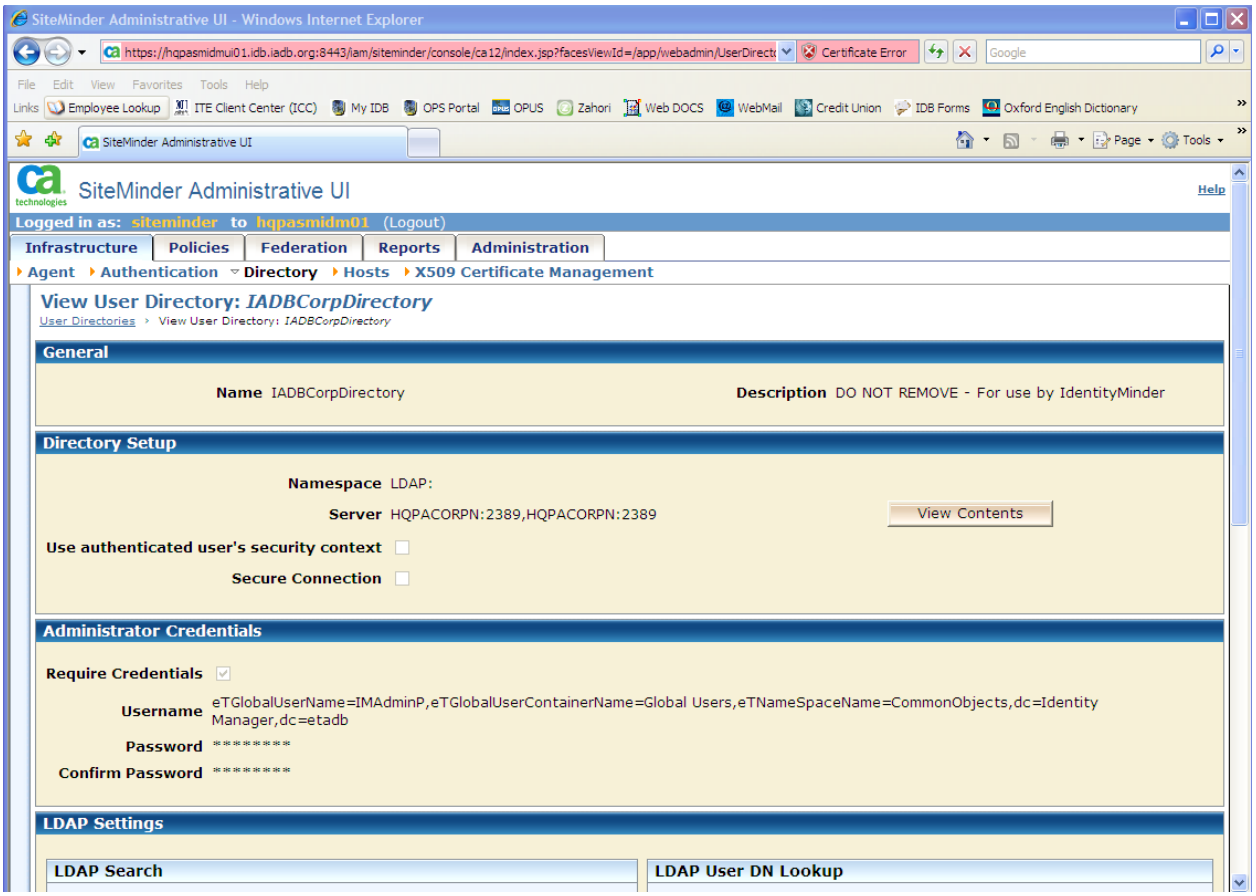
16.2 Rendimiento del Directorio de Operaciones LDAP

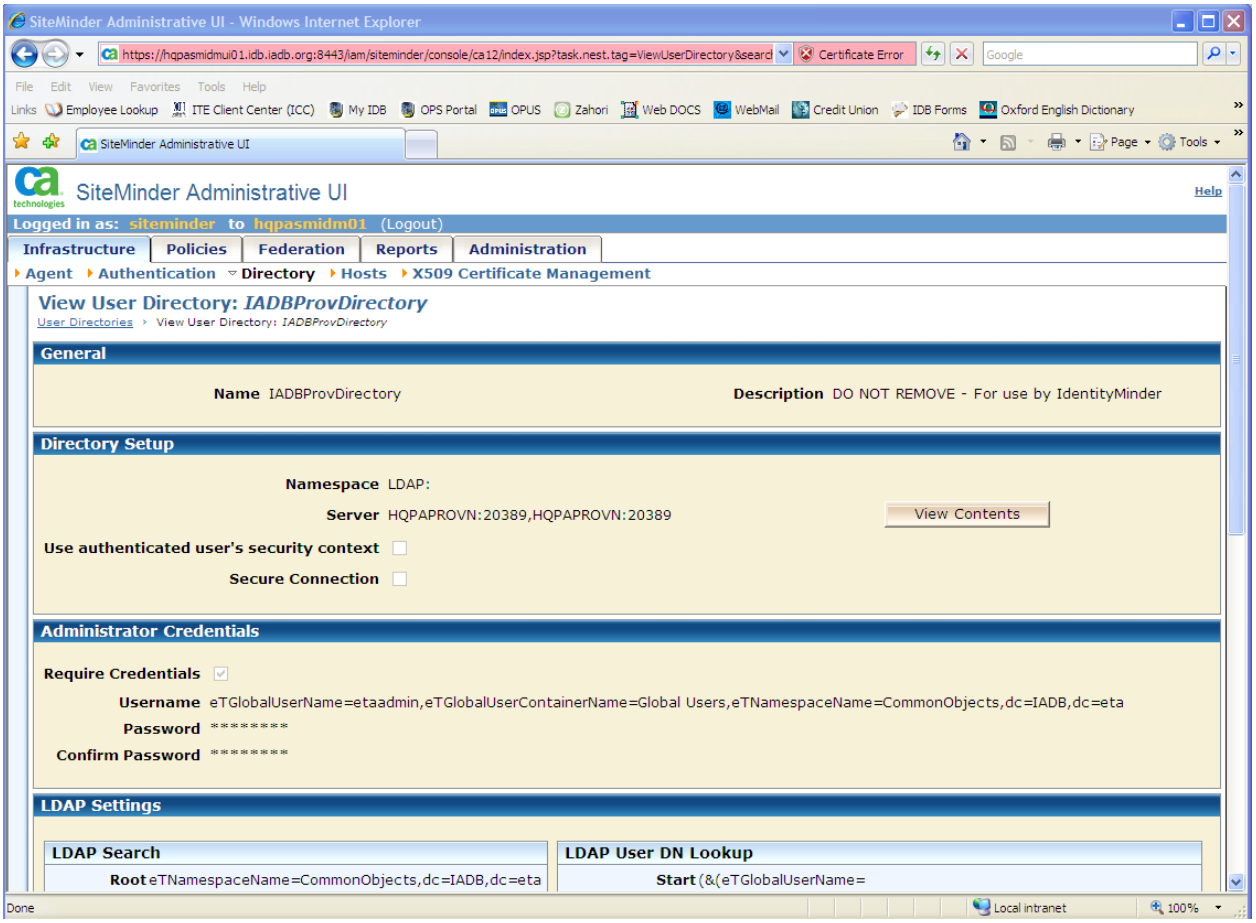
Operaciones de directorio pueden tomar más tiempo para procesar todas las solicitudes porque Identidad Minder para el directorio de usuarios LDAP se enrutan a través de un conjunto fijo de las conexiones. Para aumentar el rendimiento de las solicitudes de Identidad Minder en el directorio de usuario, configurar SiteMinder para abrir múltiples conexiones a un mismo directorio. Para ello, agregue el servidor LDAP varias veces en el directorio LDAP de conmutación por error y carga cuadro de diálogo Configuración Equilibrio en la interfaz de usuario del servidor de políticas. El número de veces para entrar en el servidor LDAP (y el número de conexiones para crear) dependerá de la carga sobre Identity Minder.

Actualmente el rendimiento se establece en óptimo con servidor LDAP añadieron 2 veces

Inicia sesión para consola de usuario de SiteMinder, abierto las propiedades del directorio de usuario -> directorio setup-> servidor-> configure

Instantánea de abajo





27.2 Usuario de conjunto de afinación

Tuning store Usuario implica una serie de pasos, entre ellos los siguientes:

• Optimización de la estructura del almacén de usuario

• Puesta a punto subyacente tiendas

• La implementación de balanceo de carga y la replicación

Estos pasos dependen del tipo de almacén de usuario que está utilizando. Para afinar la información en estas áreas, consulte la documentación de la base de datos o directorio que contiene el almacén de usuarios.

Además de las consideraciones de ajuste generales, las siguientes consideraciones de ajuste son específicos de CA IdentityMinder:

• El rendimiento de búsqueda almacén de usuarios Medida

Para un rendimiento óptimo, CA política IdentityMinder búsquedas evaluación deben completar dentro de 10-20 milisegundos.

Para asegurar que CA IdentityMinder puede completar consistentemente estas búsquedas en el tiempo recomendado, considere probar el rendimiento de búsqueda bajo múltiples condiciones de carga.

También puede utilizar esta medida para determinar cuando un almacén de usuario llega a sus límites físicos y se requieren servidores adicionales para equilibrar la carga.

• atributos índice

Índice de cada atributo que se utiliza en una política de papel o la política de identidad. Atributos de indexación pueden proporcionar importantes mejoras de rendimiento.

Nota: Para obtener información acerca de los atributos de indexación, consulte la documentación para el directorio LDAP o base de datos relacional que contiene el almacén de usuarios.

• Se liga LDAP caché

En CA IdentityMinder, todos los une directorio LDAP son ejecutados por el usuario proxy definido en el objeto CA IdentityMinder Directory. Para cada conexión, el mismo enlace LDAP se produce para este mismo usuario en repetidas ocasiones.

Si está usando un directorio LDAP como un almacén de usuarios, configurar el directorio para

 261

almacenar en caché enlaces LDAP (o sesiones), si el directorio soporta.

• Habilitar tiendas usuario cachés

Cuando CA IdentityMinder evalúa las decisiones de política para un usuario, que la información se almacena en una memoria caché de autorización. Cuando expire la información almacenada en caché, CA IdentityMinder evalúa todas las políticas para ese usuario nuevo.

Para mejorar el rendimiento de las tiendas usuario búsquedas en las evaluaciones de la regla de política posteriores, permitirá a la tienda de usuario caché buscó datos, si su tienda de usuario soporta.

CA Directory incluye una memoria caché, llamada dxCache, que es una aplicación de base de datos en memoria que se puede buscar a través de los datos almacenados en caché.

Nota: Para más información sobre CA Directory, consulte la Guía del administrador de CA Directory.

27.2.1 Cache LDAP ligas

En Identity Minder , todos los une directorio LDAP son ejecutados por el usuario proxy definido en el objeto Identidad MinderDirectory . Para cada conexión , el mismo enlace LDAP se produce para este mismo usuario en repetidas ocasiones . Configurar el directorio de caché de enlaces LDAP (o sesiones) véase CA La Guía del administrador.

Imadminp usuario se utiliza para conectarse a Corporate tienda

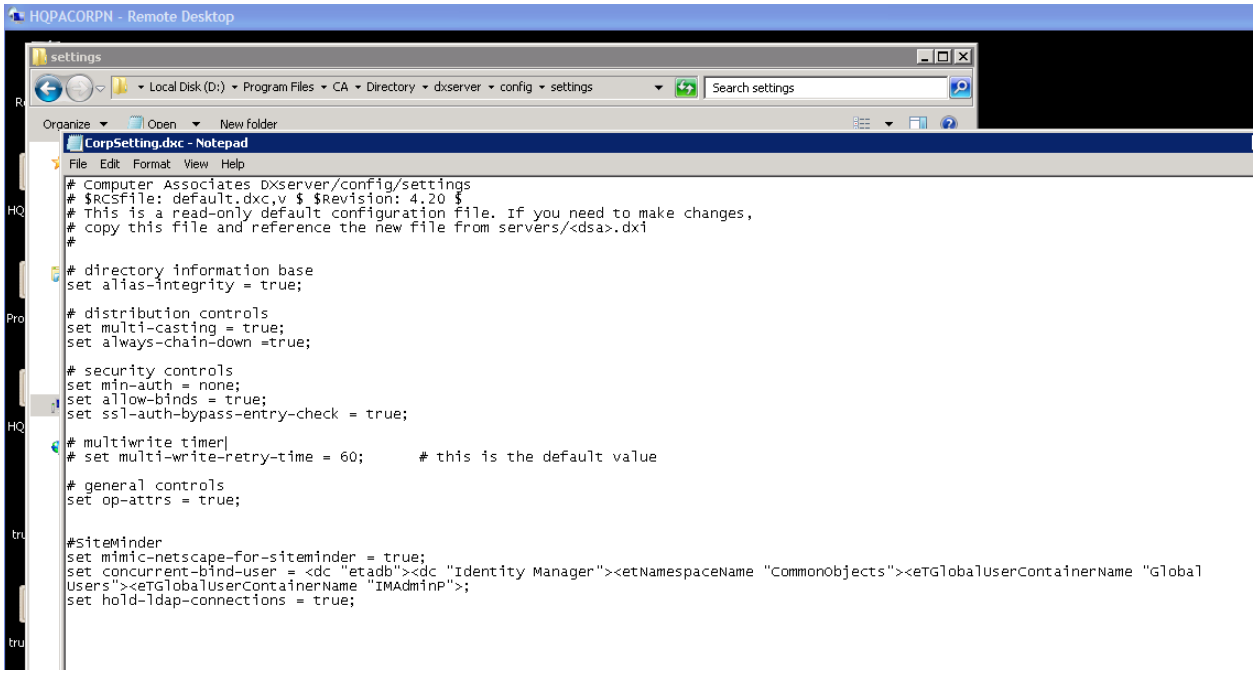
Etaadmin usuario se utiliza para conectarse a Provisioning tienda

LDAP caché liga

D : \ Archivos de programa \ CA \ Directorio \ dxserver \ config \ ajustes

Cache LDAP Binds

D:\Program Files\CA\Directory\dxserver\config\settings



set concurrent-bind-user = <dc "etadb"><dc "Identity Manager"><etNamespaceName "CommonObjects"><eTGlobalUserContainerName "Global Users"><eTGlobalUserContainerName "IMAdminP">;

27.2.2 Activar tiendasa usuario caché

Cuando Identidad Minderevaluates las decisiones de política para un usuario , que la información se almacena en una memoria caché de autorización. Cuando la información almacenada

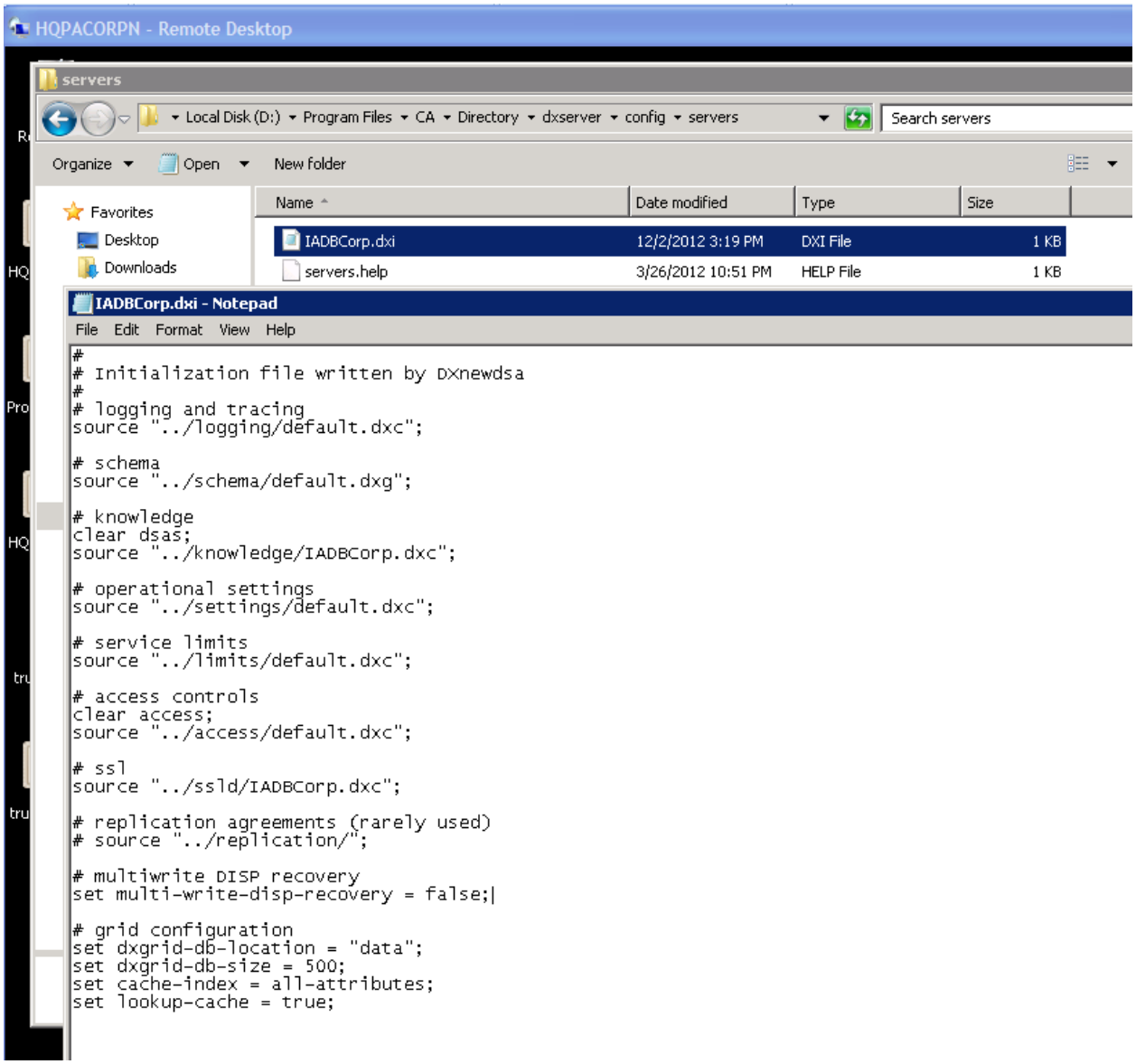
en caché caduca , Identidad Minderevaluates todas las políticas para ese usuario nuevo.

Para mejorar el rendimiento de las tiendas usuario búsquedas en las evaluaciones de la regla de política posteriores , permitirá a la tienda de usuario caché buscó datos.

Editar archivo de inicialización de la instancia de directorio para el ajuste de configuración de la caché

Directorio de \ Archivos de programa \ CA \ eTrust \ dxserver \ config \ servers \ IADBCorp.dxi : D

D:\Program Files\CA\Directory\dxserver\config\servers



27.2.3 Ajuste para los componenetes de aprovisionamiento

Las siguientes optimizaciones se utilizan para asegurar el mejor rendimiento :

■ Optimizar la conexión entre el servidor de Identidad Minder y el servidor de aprovisionamiento

Identidad Minder se comunica con el servidor de aprovisionamiento mediante la API de Java IAM (JIAM) . Para mejorar el rendimiento de comunicación , configure lo siguiente:

- Piscina sesión JIAM para múltiples conexiones con el servidor de aprovisionamiento

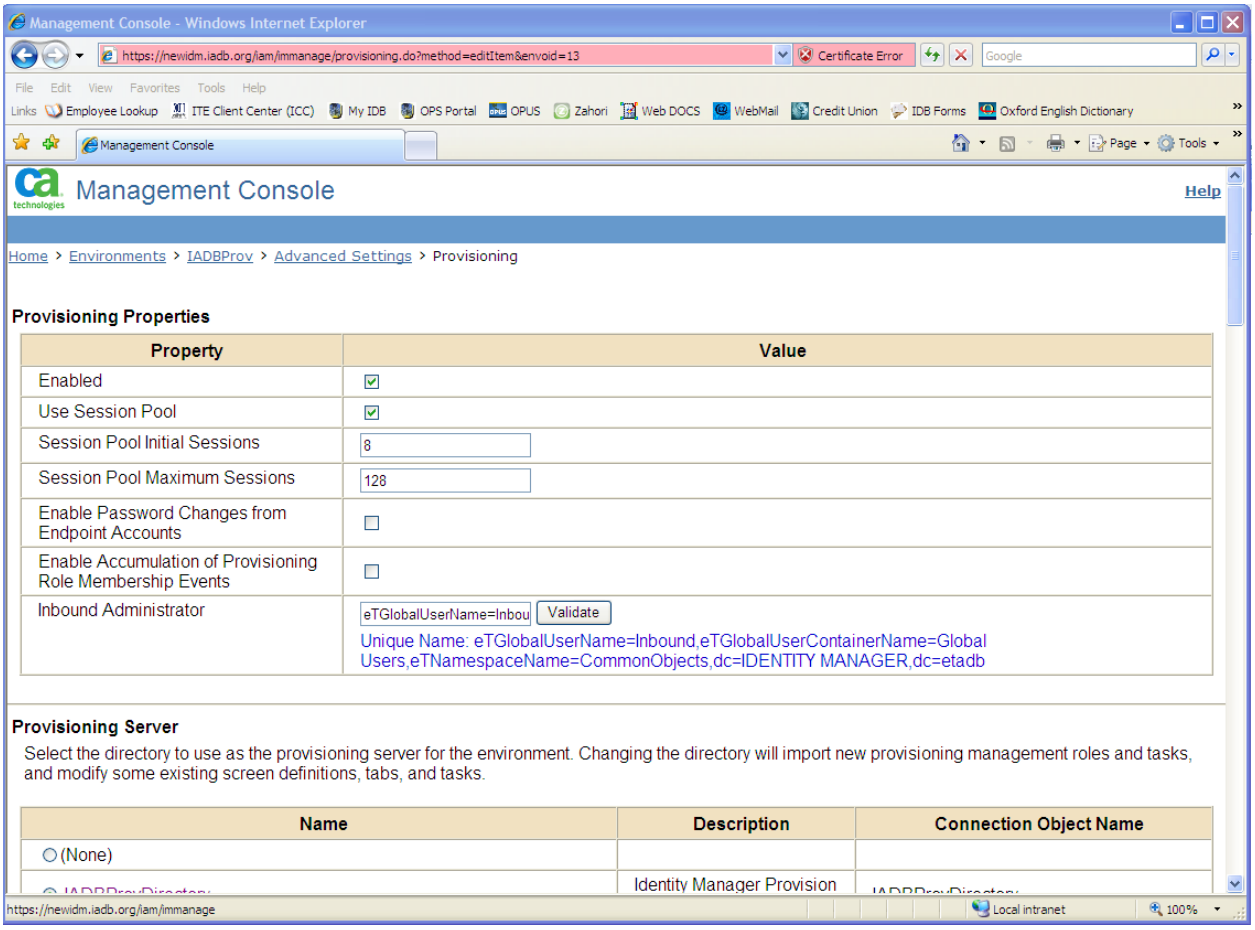
Nota : CA recomienda establecer el valor de las sesiones iniciales de 8 , y las sesiones máximas a 128 .

- Caché JIAM para objetos recuperados del servidor de aprovisionamiento

Inicia sesión para IM Management Console

Busque con entorno > IADBProv- > Avanzado Preferencias- > Aprovisionamiento

Ajustar la configuración de la piscina sesión



■ Set de sincronización cuenta que se produzca al final de una tarea en lugar de al final de cada evento

■ Sintonice el servidor de aprovisionamiento

Nota: Consulte la Guía de Aprovisionamiento y Guía de alta disponibilidad para más información.

La producción está sintonizado a la configuración recomendada como abajo :

27.2.4 Puesta a punto de Indetity Minder en base de datos

Cuando la ejecución de tareas, Identidad Minder utiliza las siguientes bases de datos:

■ persistencia de tareas

Mantiene la información sobre las tareas de Identidad Minder y eventos a través del tiempo. Esto permite Identidad Minder para restaurar el último estado conocido de eventos y tareas en el caso de fallo del sistema.

Nota: Esta base de datos tiene el impacto más significativo en el rendimiento de identidad Minder porque la tarea y sus eventos se guardan y se recuperan de la base de datos durante las transiciones de estado.

■ Auditoría

Proporciona un registro histórico de las operaciones que se producen en un entorno de Identidad Minder.

■ Flujo de trabajo

Tiendas Flujo de trabajo de definiciones de procesos, trabajos, guiones y otros datos requeridos por el motor de flujo de trabajo.

267

■ Informes

Tiendas instantánea de datos, lo que refleja el estado actual de los objetos en Identidad Minder en el momento en que se toma la instantánea. Identidad Minder comunica con cada base de datos a través de un conjunto de conexiones JDBC. Puede crear y configurar una agrupación de conexiones JDBC en el servidor de aplicaciones que aloja Identidad Minder. Al configurar la agrupación de conexiones JDBC, tenga en cuenta lo siguiente:

■ Considere el número de tareas concurrentes que se ejecutarán en un momento dado.

■ Considere los otros componentes de tiempo de ejecución al configurar el tamaño de la agrupación de conexiones JDBC. Cada componente de tiempo de ejecución funciona en conjunción con los otros componentes de tiempo de ejecución.

Nota: CA recomienda establecer el valor inicial de agrupación de conexiones a 128.

■ Para la base de datos de persistencia de tareas, el número de conexiones de base de datos en la piscina debe permitir la ejecución de cada tarea para recuperar y actualizar datos de tareas y eventos a lo largo del tiempo de vida de la tarea.

■ La base de datos de persistencia tarea usa comandos preparados. Asegúrese de configurar la caché declaración preparada para la base de datos que está utilizando para almacenar datos de persistencia de tareas.

Nota: Consulte la documentación de la base de datos que está utilizando para la persistencia de tareas para obtener información sobre la configuración de la caché declaración preparada.

Ajustes de producción son:

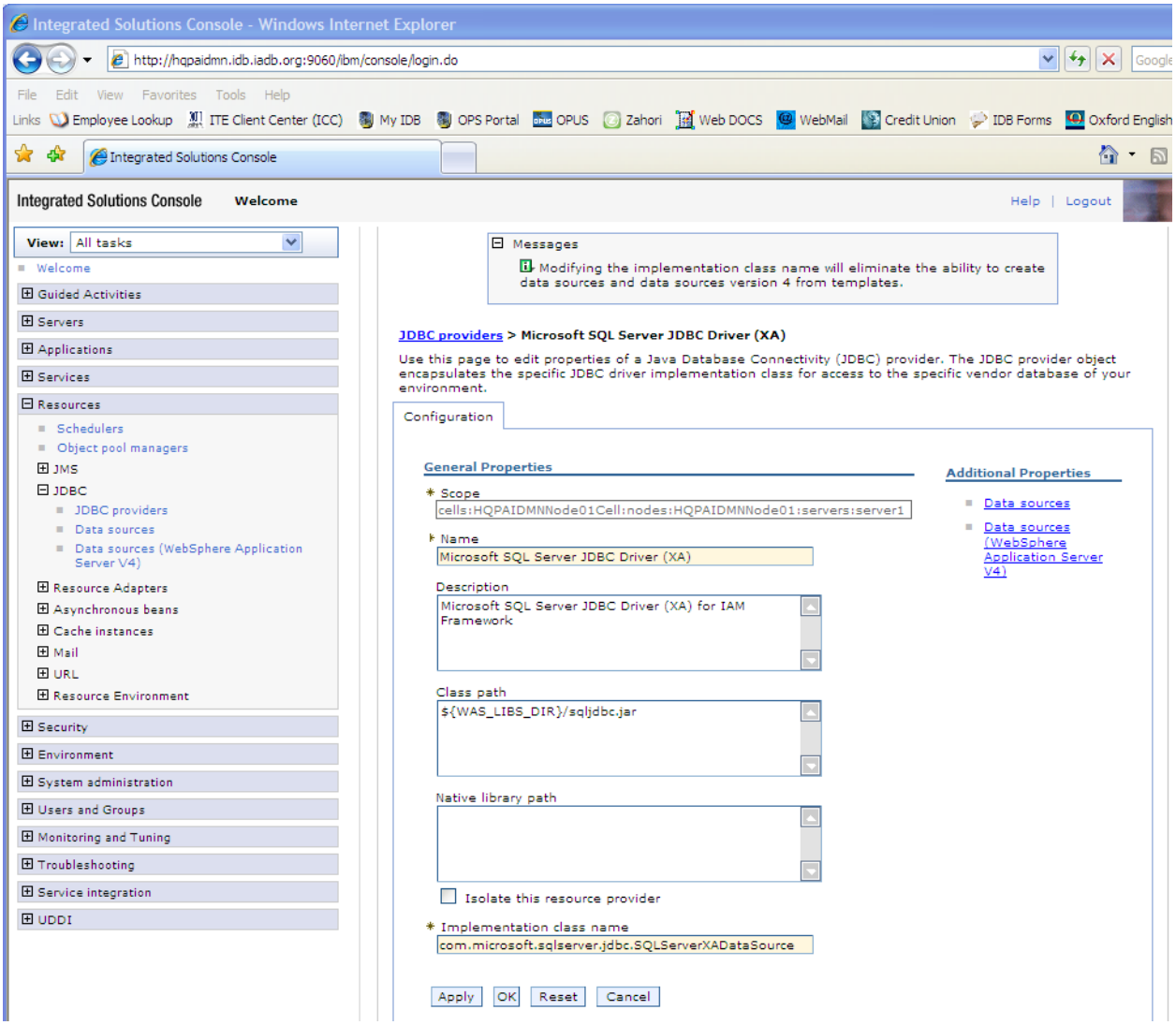
Inicia sesión para consola de administración de IBM Websphere

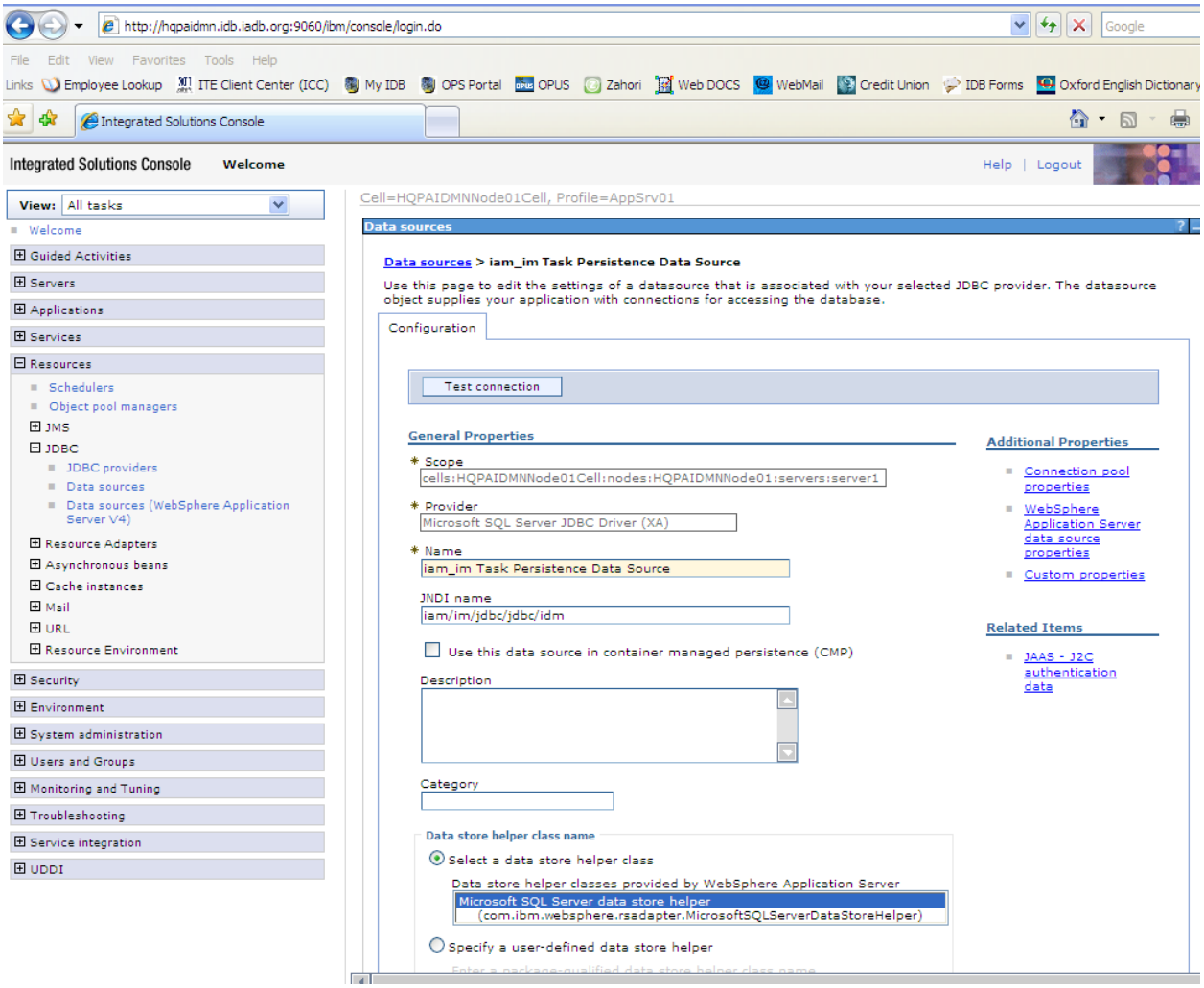
http://hqpaidmn.idb.iadb.org:9060/ibm/console

Examinar para Recursos-> JDBC-> Orígenes de datos

Seleccione datasoure

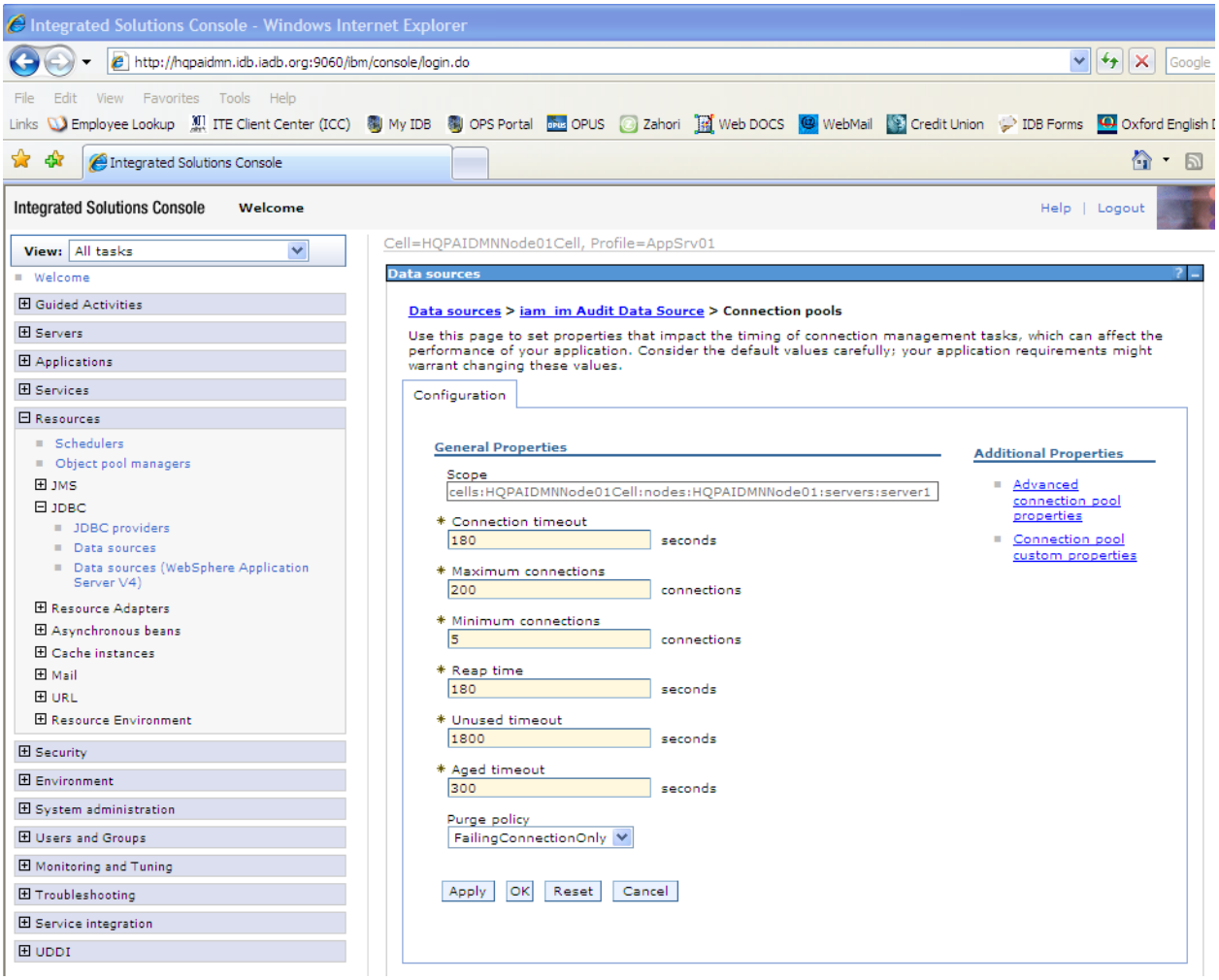
269


Integrated Solutions Console - Windows Internet Explorer
http://hqpaidmn.idb.iadb.org:9060/ibm/console/login.do
File Edit View Favorites Tools Help
Links Employee Lookup ITE Client Center (ICC) My IDB OPS Portal OPUS Zahori Web DOCS WebMail Credit Union IDB Forms Oxford English
Integrated Solutions Console
Integrated Solutions Console Welcome
Help | Logout
View: All tasks
Welcome
Guided Activities
Servers
Applications
Services
Resources
Schedulers
Object pool managers
JMS
JDBC
JDBC providers
Data sources
Data sources (WebSphere Application Server V4)
Resource Adapters
Asynchronous beans
Cache instances
Mail
URL
Resource Environment
Security
Environment
System administration
Users and Groups
Monitoring and Tuning
Troubleshooting
Service integration
UDDI
Messages
Modifying the implementation class name will eliminate the ability to create data sources and data sources version 4 from templates.
JDBC providers > Microsoft SQL Server JDBC Driver (XA)
Use this page to edit properties of a Java Database Connectivity (JDBC) provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment.
Configuration
General Properties
Scope
cells:HQPAIDMNNode01Cell:nodes:HQPAIDMNNode01:servers:server1
Name
Microsoft SQL Server JDBC Driver (XA)
Description
Microsoft SQL Server JDBC Driver (XA) for IAM Framework
Class path
${WAS_LIBS_DIR}/sqljdbc.jar
Native library path
Isolate this resource provider
Implementation class name
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
Apply OK Reset Cancel
Additional Properties
Data sources
Data sources (WebSphere Application Server V4)



selecciona propiedades de conexión

271



Realice estos pasos para todas las Fuentes de datos para sincronizar.

27.2.5 Sincronizar JVM

1. Iniciar secion para consola WebSphere de IBM

Prueba :

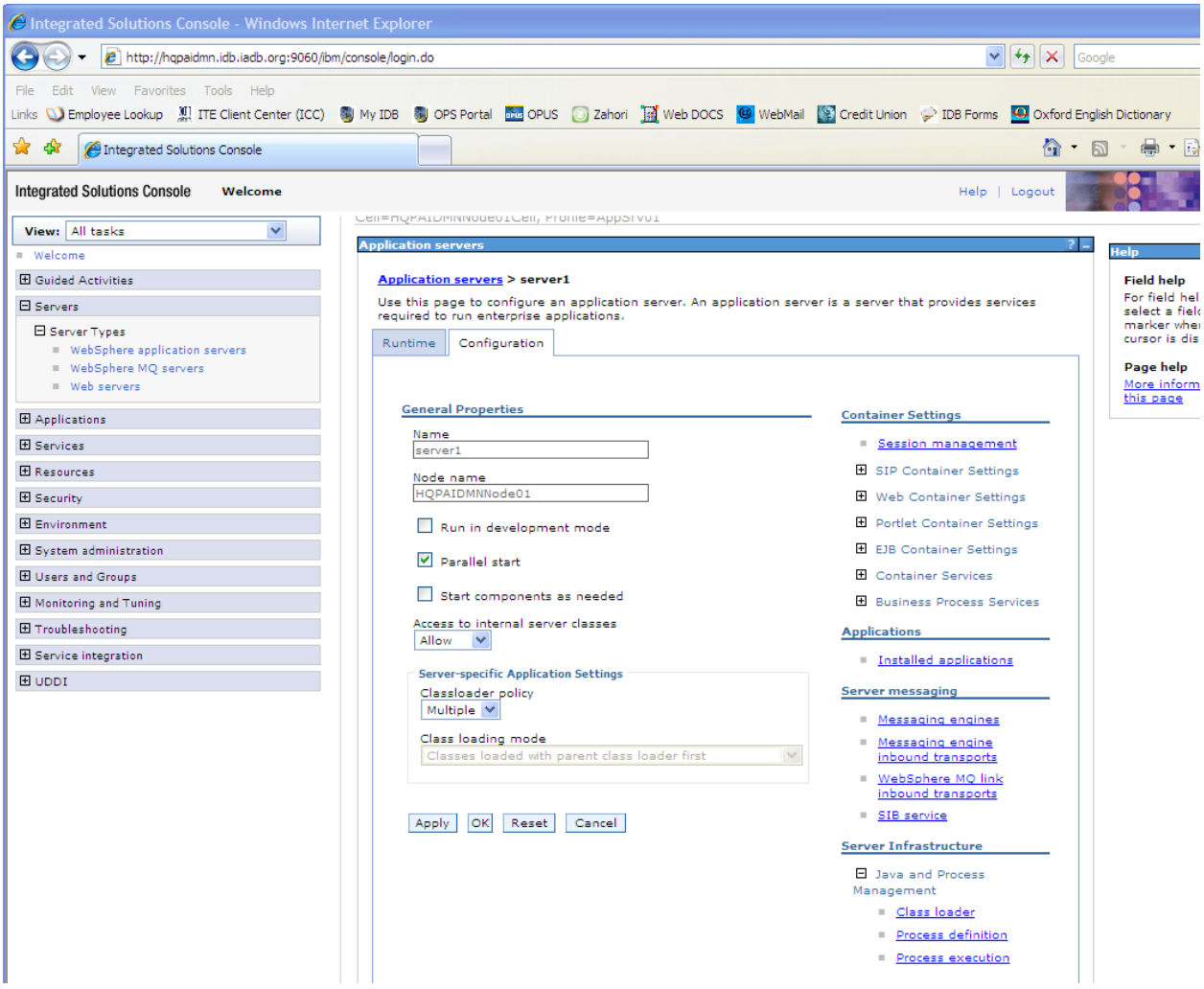
http://hqdaidmn.idb.iadb.org:9060/ibm/console

Producción:

http://hqpaidmn.idb.iadb.org:9060/ibm/console

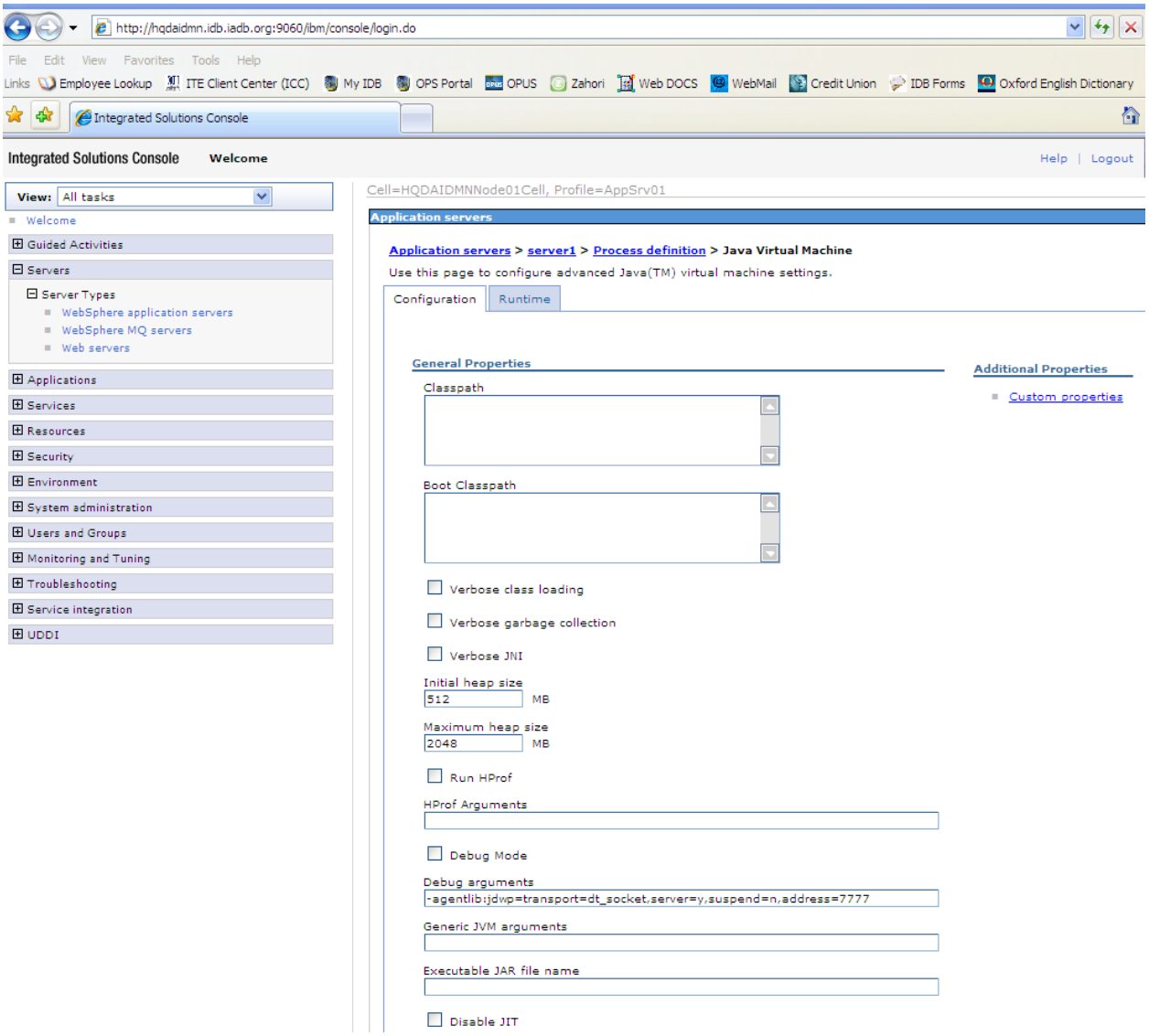
2. Navegar con

Servers->Application Servers->Server1->Process Definition (Java and Process Management)->Java Virtual Machine



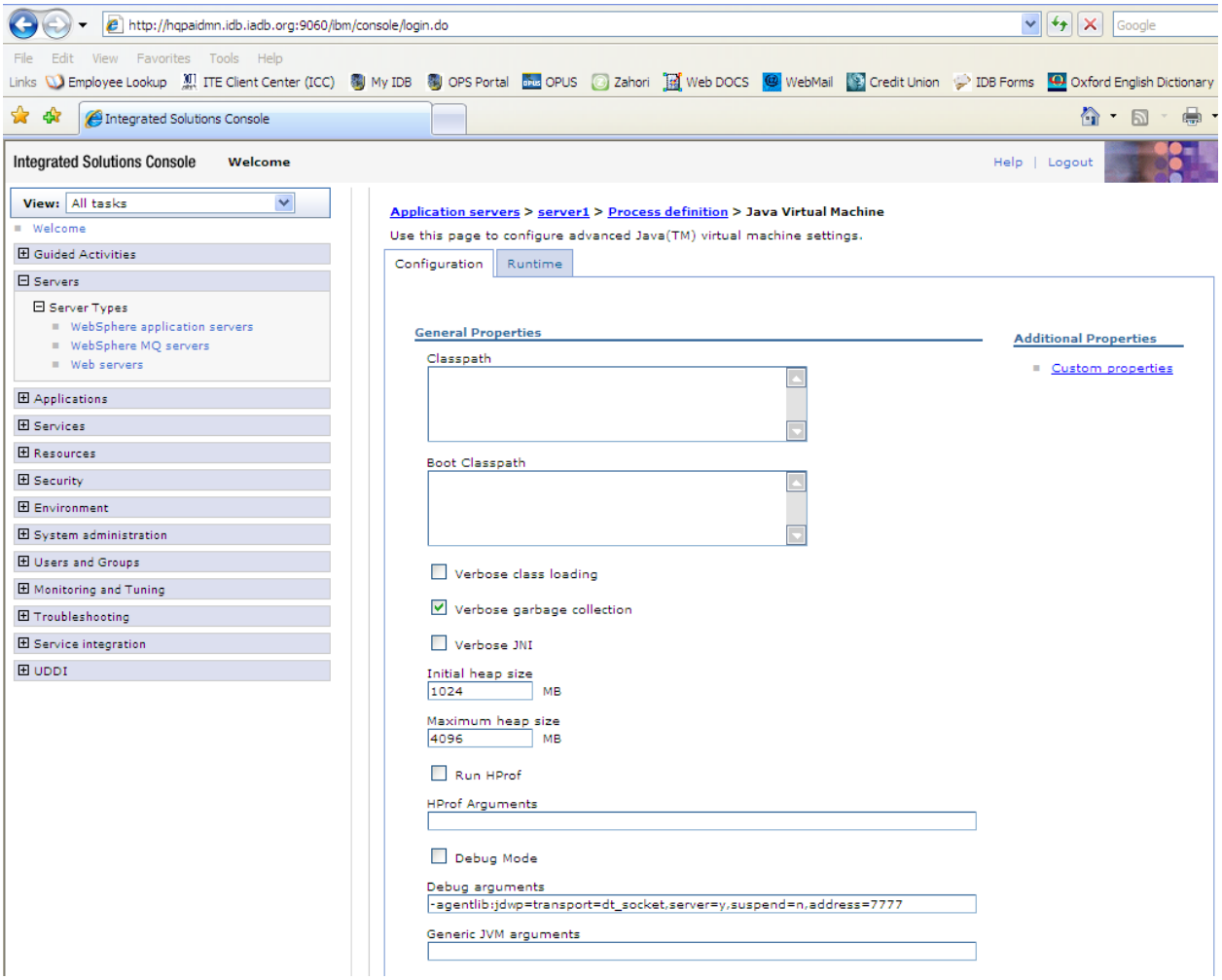
A continuación esta la creación del entorno de prueba

273



A continuación los ajustes realizados en el entorno de producción

274



el tamaño de pila de JVM es la que necesita la configuración si ve alguna fuera de errores de memoria de JVM , un administrador de WebSphere puede configurar otras opciones de JVM avanzado si es necesario

27.2.6 Proceso de limpieza de basura (Audit DB)

(Check IDM guide r12.6 for more details.)

Cuando usted necesita para limpiar los datos antiguos de la base de datos de auditoría siguiente es el procedimiento :

Existe un procedimiento " garbageCollectAuditing125 " en IMSTORE (almacén de datos para IM) . Este procedimiento almacenado se debe ejecutar para eliminar los datos antes de la fecha especificada.

garbageCollectAuditing125 entorno nombre DD / MM / AAAA

entorno de nombre-

Define el nombre del entorno de Identity Manager

AAAA- MM- DD (en SQL Server se puede dar con la marca de tiempo)

Define la fecha antes de la cual los registros de auditoría deben ser eliminados.

En SQL Server:

Ejemplo: exec dbo.garbageCollectAuditing125 Identity_Manager , ' 2011-09-29 04 : 04 : 37,747
'

27.2.7 Proceso de limpieza de basura (tareas persistentes)

Cuando usted necesita para limpiar los datos antiguos de la base de datos de persistencia tarea siguiente es el procedimiento :

Existe un procedimiento " garbageCollectTaskPersistence " en IMSTORE (almacén de datos para IM) . Este procedimiento almacenado se debe ejecutar para eliminar los datos antes de la fecha especificada.

garbageCollectTaskPersistence entorno nombre DD / MM / AAAA

entorno de nombre

Define el nombre del entorno de Identity Manager

AAAA- MM- DD (en SQL Server se puede dar con la marca de tiempo)

Define la fecha antes de la cual los registros de auditoría deben ser eliminados.

En SQL Server:

Ejemplo: exec dbo.garbageCollectTaskPersistense Identity_Manager , ' 2011-09-29 04 : 04 : 37,747 '

277

27.3 Appendix A: Instalar/Actualizar Provisionamiento de administrador de clientes (Refer SIS document)

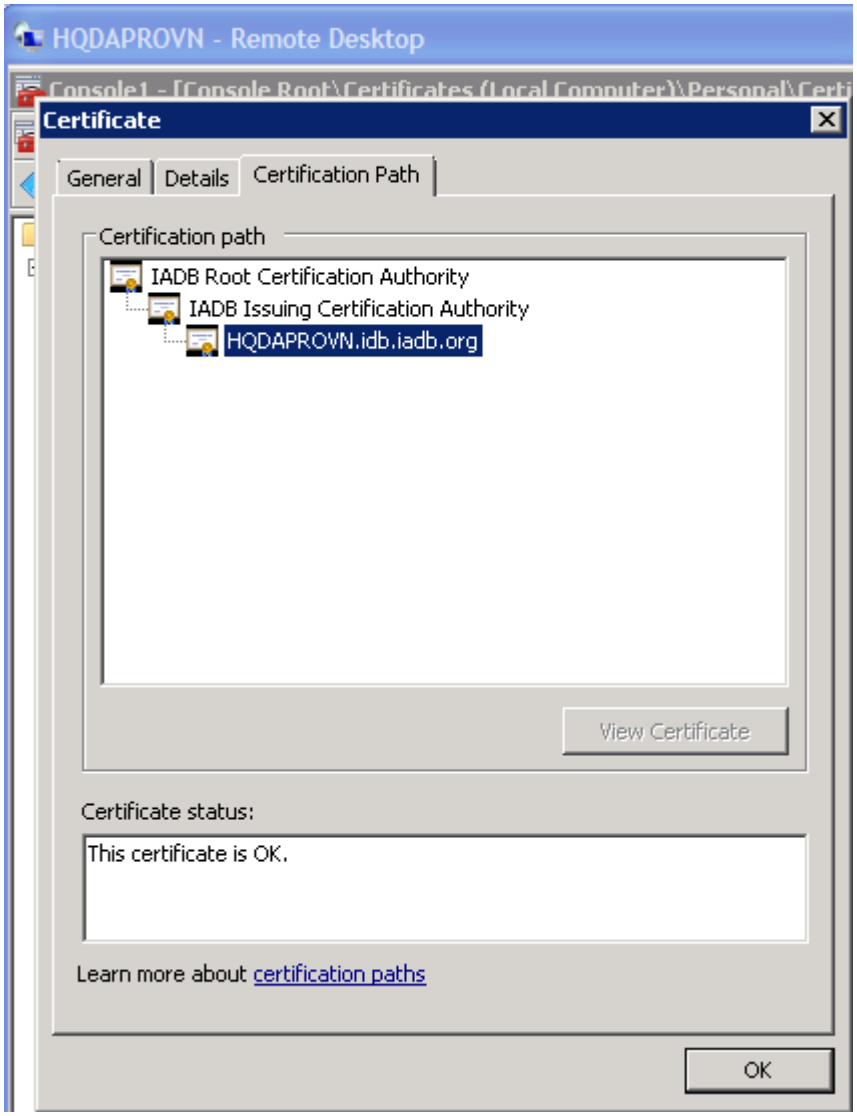
27.4 Appendix B: Importacion de certificados de Active Directory

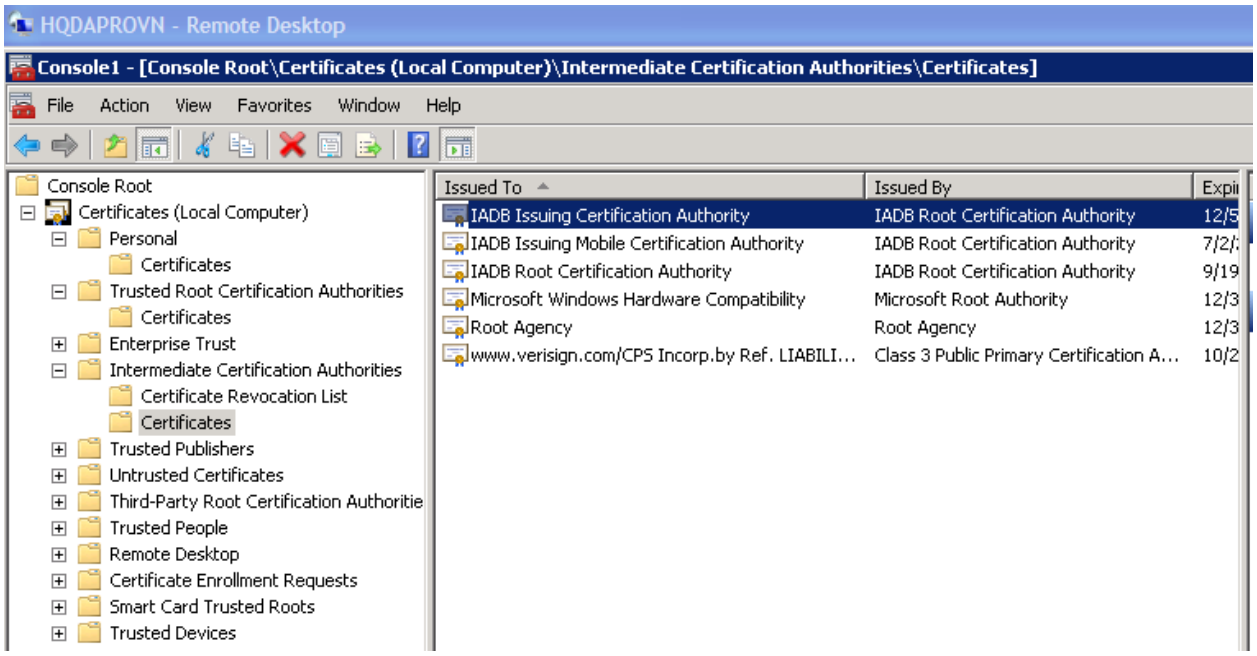
Provisioning Server necesita los siguientes 2 sólo certificados de CA raíz

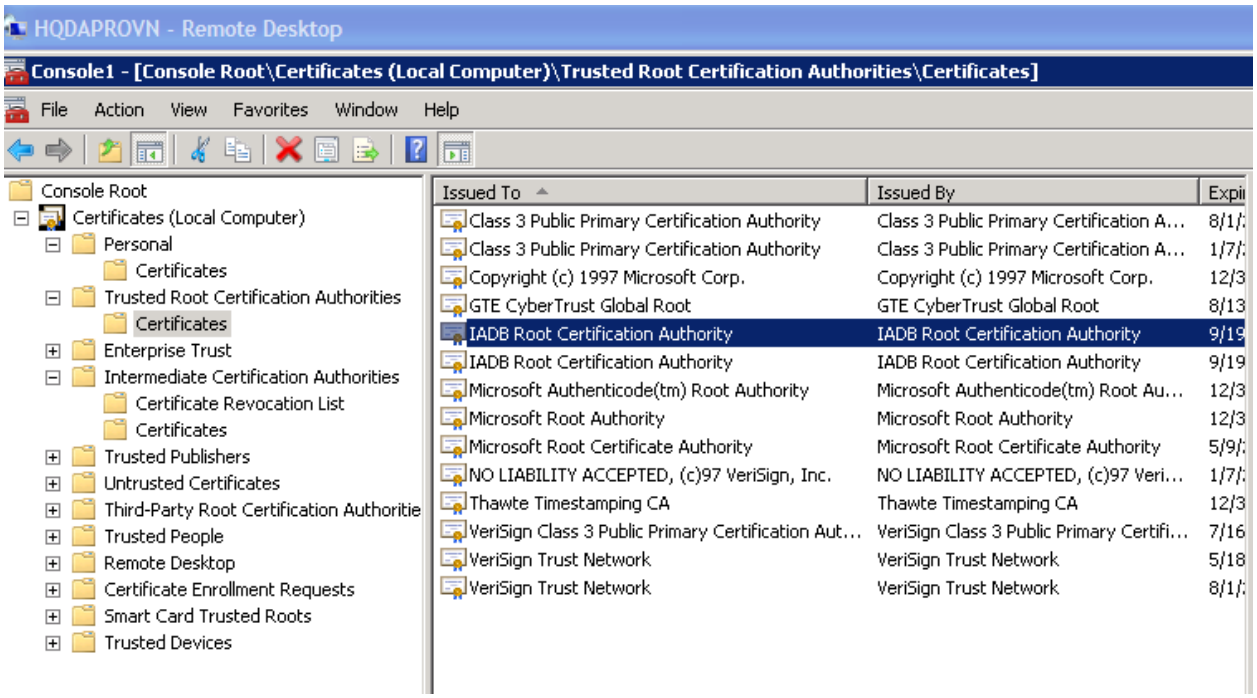
• Autoridad de Certificación Raíz BID

• BID Emisión Autoridad de Certificación

Browse to the folder for server certificates




HQDAPROVN - Remote Desktop
Console1 - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoritie
Trusted People
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Issued To
Issued By
Expi
IADB Issuing Certification Authority
IADB Root Certification Authority
12/5
IADB Issuing Mobile Certification Authority
IADB Root Certification Authority
7/2/
IADB Root Certification Authority
IADB Root Certification Authority
9/19
Microsoft Windows Hardware Compatibility
Microsoft Root Authority
12/3
Root Agency
Root Agency
12/3
www.verisign.com/CPS Incorp.by Ref. LIABILI...
Class 3 Public Primary Certification A...
10/2


HQDAPROVN - Remote Desktop
Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authoritie
Trusted People
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Issued To
Issued By
Expi
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification A...
8/1/
Class 3 Public Primary Certification Authority
Class 3 Public Primary Certification A...
1/7/
Copyright (c) 1997 Microsoft Corp.
Copyright (c) 1997 Microsoft Corp.
12/3
GTE CyberTrust Global Root
GTE CyberTrust Global Root
8/13
IADB Root Certification Authority
IADB Root Certification Authority
9/19
IADB Root Certification Authority
IADB Root Certification Authority
9/19
Microsoft Authenticode(tm) Root Authority
Microsoft Authenticode(tm) Root Au...
12/3
Microsoft Root Authority
Microsoft Root Authority
12/3
Microsoft Root Certificate Authority
Microsoft Root Certificate Authority
5/9/
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.
NO LIABILITY ACCEPTED, (c)97 Veri...
1/7/
Thawte Timestamping CA
Thawte Timestamping CA
12/3
VeriSign Class 3 Public Primary Certification Aut...
VeriSign Class 3 Public Primary Certifi...
7/16
VeriSign Trust Network
VeriSign Trust Network
5/18
VeriSign Trust Network
VeriSign Trust Network
8/1/

Guia del Paquete SSIS PSFEED

Introducción

1.1 Proposito

El propostio de este document es hacer una lista paso a paso el proceso y las directrices a seguir por un official de seguridad de la Información, para modificar o solucionar cualquier asunto relacionado con el paquete SSIS PSDFEED.

1.2 Alcance de los servicios

Solución de problemas del paquete de datos

Las modificaciones y adiciones al procedimiento.

1.3 Fuera de servicios del alcance

Sube al servidor, el funcionamiento y la programación del SQL Job

2 Paisaje de tecnologia

1. MS SQL Server 2008

2. MS SQL servidor Business intelligence development studio 2008

3 Procedimientos operativos

Job Name: CAIM126_IADBPSFEED1 (Package)

2) SSIS Estructura del paquete

El paquete SSIS tiene el propósito de proveer los acontecimientos de personas que entran / salir del banco , así como cambios en los registros de las personas con contratos válidos en el sistema de Recursos Humanos (PeopleSoft) de seguridad de la información para tomar las medidas necesarias en base a la interna Controles, los eventos son nuevos usuarios , Usuarios recontratados , Usuarios terminados , Usuarios transferidas , Gerentes Actualizado . Estos eventos están separados

básicamente en dos tipos: STAFF and NON-STAFF.

El paquete fue desarrollado originalmente en una infraestructura de SQL 2000 (paquete DTS) , se configura actualmente en SQL 2008 (paquete SSIS) .

Los componentes en el interior del paquete SSIS se especifican en el siguiente documento : SSIS PSFEED TABLE

Checar la tabla SSIS PSFEED TABLE en Apendice

IADBPSFEED1.xlsx

El paquete está programado para correr de la siguiente manera :

Producción

Servidor: IDBPRDB2 \ IDBPRDB2INST2

Nombre del trabajo : CAIM126_IADBPSFEED1

Prueba

IDBTRDA1 \ IDBTRDA1INST1 : ETAPSDBTST (base de datos)

IDBTRDB2 \ IDBTRDB2INST2 : IADBPSFEED1 (paquete DTS)

3) EXECUCION

1. Archivo de entrada de people soft

prov_file.txt - Trabajo diario Programado 06:30am de lunes a viernes

Servidor en donde se deposita el archivo prov_file.txt, producción \\ itfectp07 \ dataprop \

Servidor en donde se deposita el archivo prov_file.txt, Prueba \\ itfectp07 \ Dataprot \

GlobalUsers archivo :

Producción \\ HQPAPROVN \ psfeed $ \ input \

GlobalUsers.csv

Prueba \\ HQDAPROVN \ psfeed $ \ input \ GlobalUsers.csv

Ejecutar paquete DTS para obtener lo siguiente: (Haga click en la DTS Trabajo y seleccione Ejecutar) que dará lugar a los siguientes archivos , que son el resultado de la lógica de los

282

procedimientos almacenados dentro del paquete SSIS . Este trabajo está programado para ejecutarse a las 07:30 am , de lunes a viernes en PROD SQL Server: IDBPRDB2 \ IDBPRDB2INST2 PRUEBA: IDBTRDB2 \ IDBTRDB2INST2 .

En caso de tener un problema con este paquete, verificar los registros con el equipo de DBA y la ejecución .

HQPAPROVN\D:\psfeed\output\STAFF

new_users_role.csv

rehired_users_role.csv

terminated_users.csv

transferred_users.csv

updated_mgrs.csv

HQPAPROVN\D:\psfeed\output\NONSTAFF

new_users_role_nonstaff.csv

rehired_users_role_nonstaff.csv

terminated_users_nonstaff.csv

transferred_users_nonstaff.csv

updated_mgrs_nonstaff.csv

HQPAPROVN\D:\psfeed\output\Exceptions

existing_users.csv

username_exception.csv

failsafe_errormessage.csv

new_users_role_faildump.csv

rehired_users_faildump.csv

terminated_users_faildump.csv

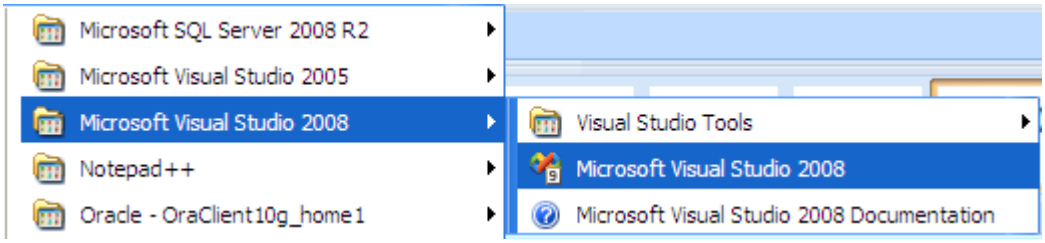
transferred_users_faildump.csv

New_users_exception.csv

Role_Dept_Missing_Exception.csv

1. Los archivos de salida son los que se usan para el proceso de aprovisionamiento diario

La herramienta utilizada para ver/actualizar el codigo Microsift Visual Studio 2008



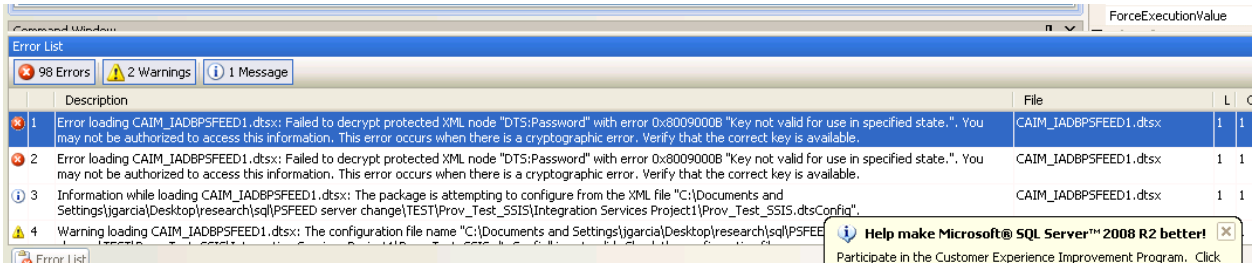
Con el fin de abrir el paquete se puede localizar el archivo en

Prov_Test_SSIS.sln \\ ITASRV1 \ D \ SQL 2005 a SQL 2008 \ SSIS_Package_TransitionJGARCIA \ TST \ PSFEED \ Prov_Test_SSIS

El paquete se carga en Microsoft Visual Studio y en caso de que muestra los errores y advertencias como los de abajo , es porque el paquete se abre en una máquina diferente a donde

284

estaba la última abierta / modificado con éxito



Estos errores / advertencias son en cuanto a dos cosas posibles :

a. El ID de cargar el paquete de Microsoft Visual Studio no tiene los permisos necesarios en las rutas especificadas en el archivo de configuración o

b . El paquete fue copiado de la ruta original , y ya que el paquete siempre trata de encontrar el archivo de configuración desde donde originalmente se guardó por última vez

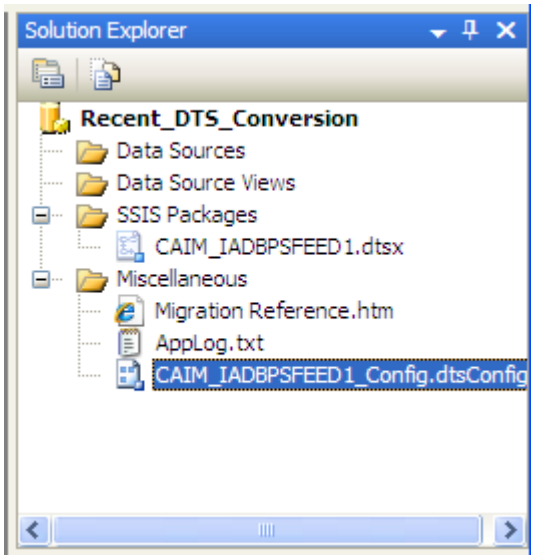
Soluciones:

Para el tipo de problema a, ID debe tener los permisos especificados en el documento adjunto

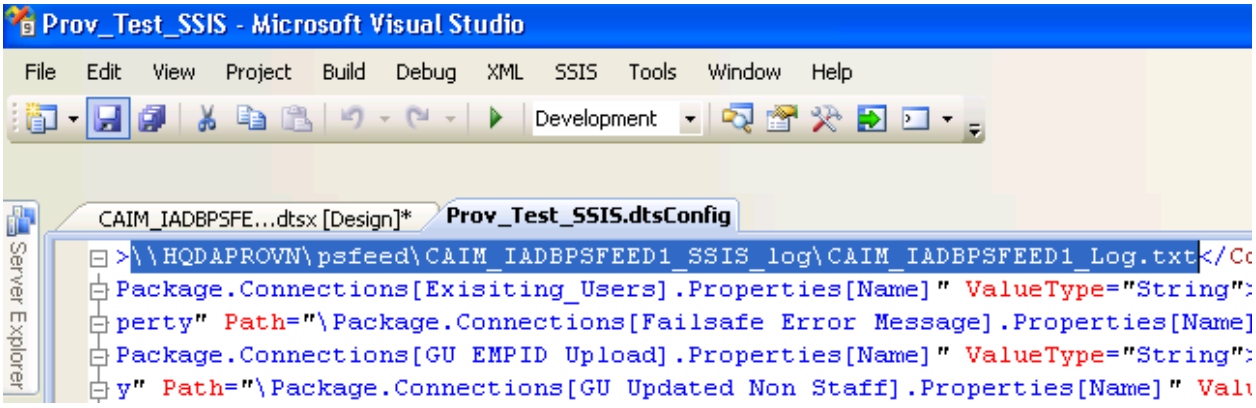
Por tipo de problema b , el paquete tiene que ser reconfigurado

2. Con el fin de reconfigurar el paquete por favor, siga los siguientes pasos :

3. Doble click en .dtsConfig archive que aparece en el lado derecho

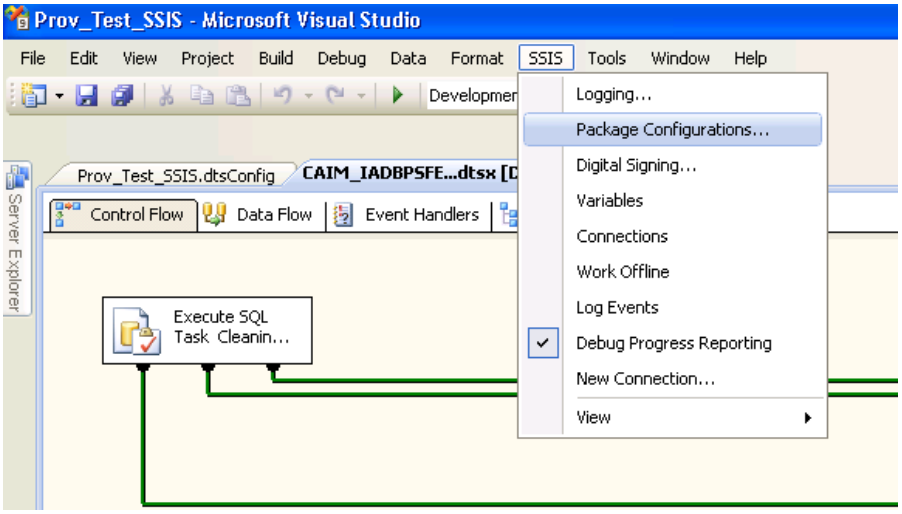


4. Vuelva a colocar todos los valores necesarios y guarder los cambios

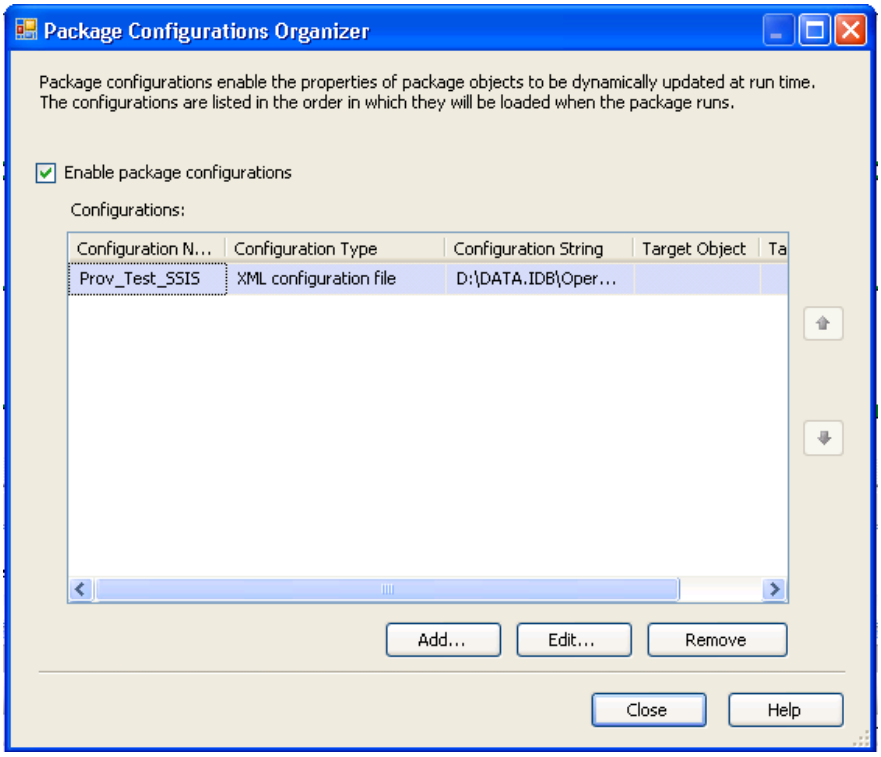


5. Haga clic en el área en blanco en la ficha Flujo de control y seleccione las configuraciones opcionales del paquete bajo el menú SSIS

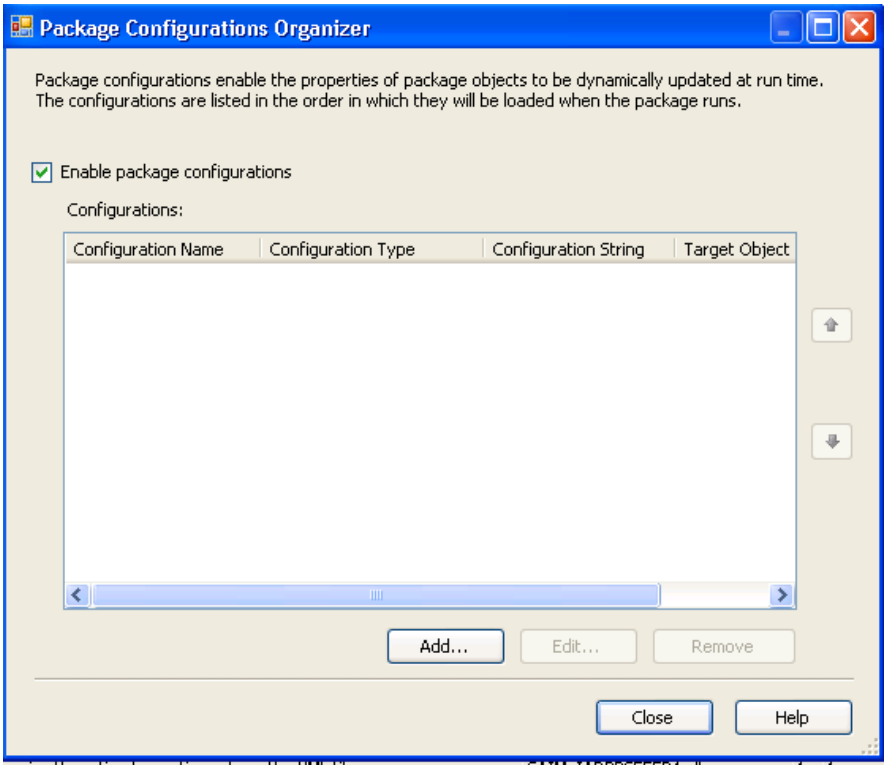
286



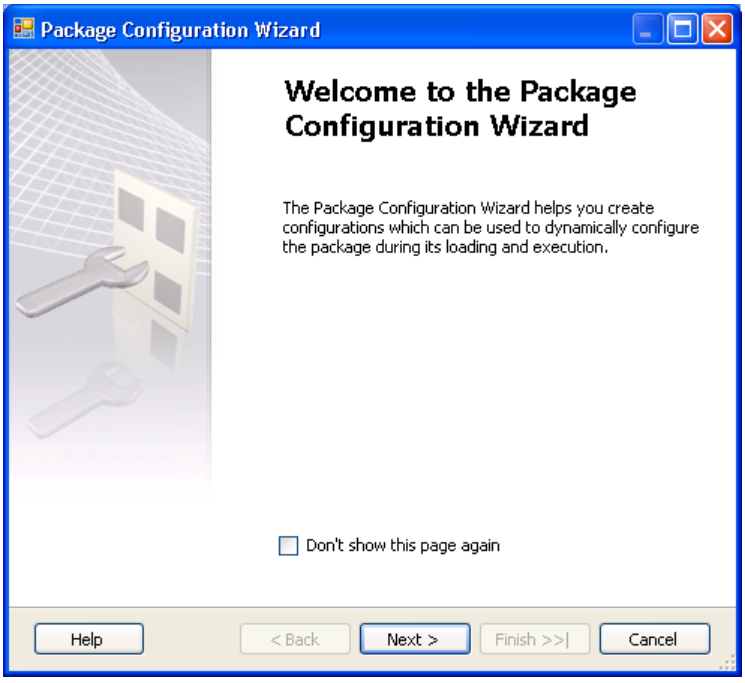
6. Selecciona para borrar



7. Las configuraciones disponibles se convertirtá en vació, haga clic en Añadir…



8. Se le permitir con el asistente para la configuración de paquetes, haga clic en siguiente>

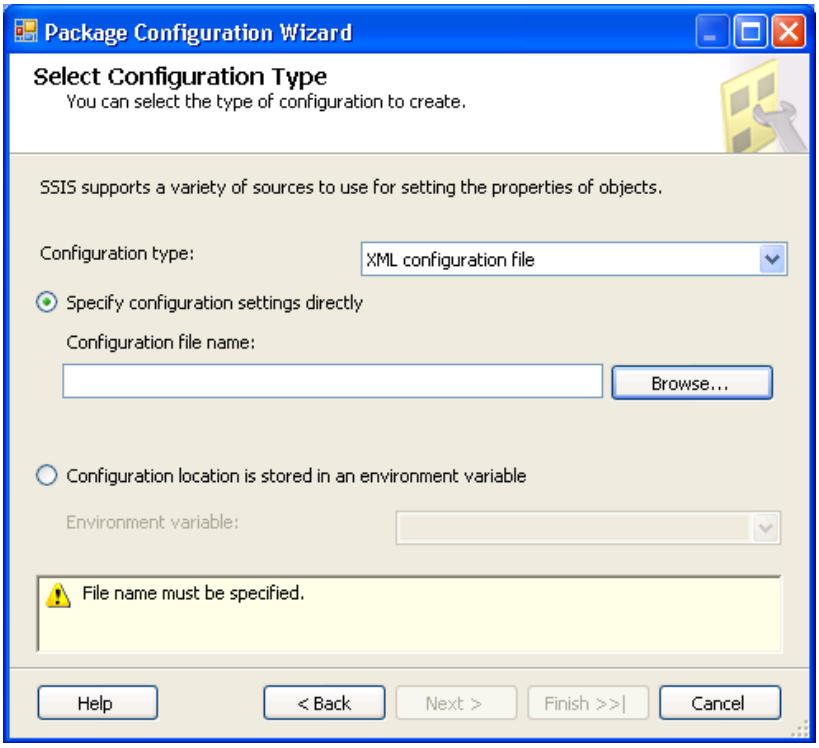


9. Elige las siguientes opciones

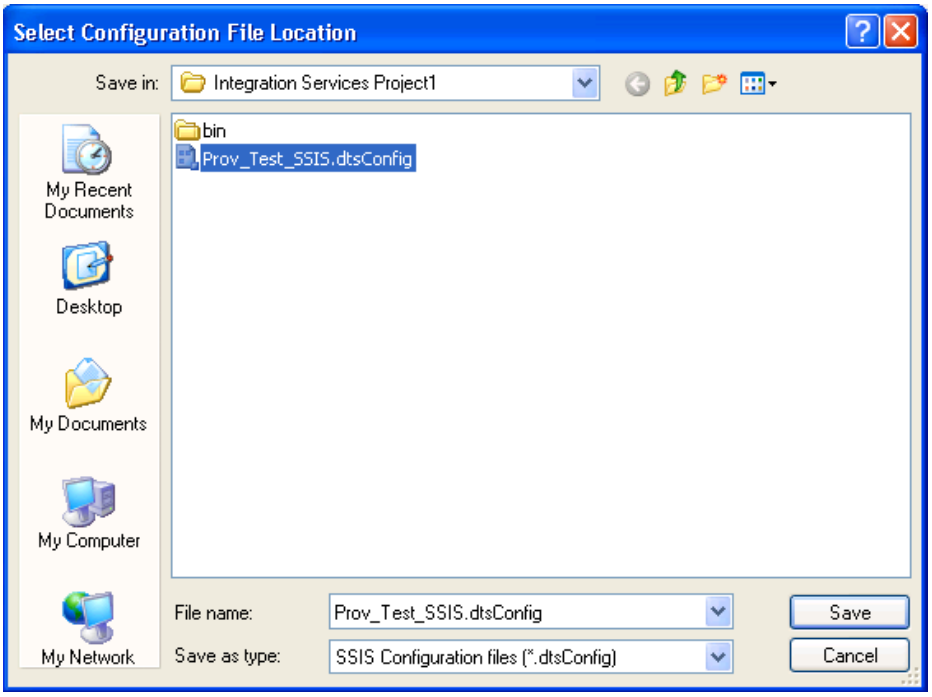
a. Tipo de configuración: XML archivo de configuraciónn

b. Especifique directamente los valores de configuraciónn

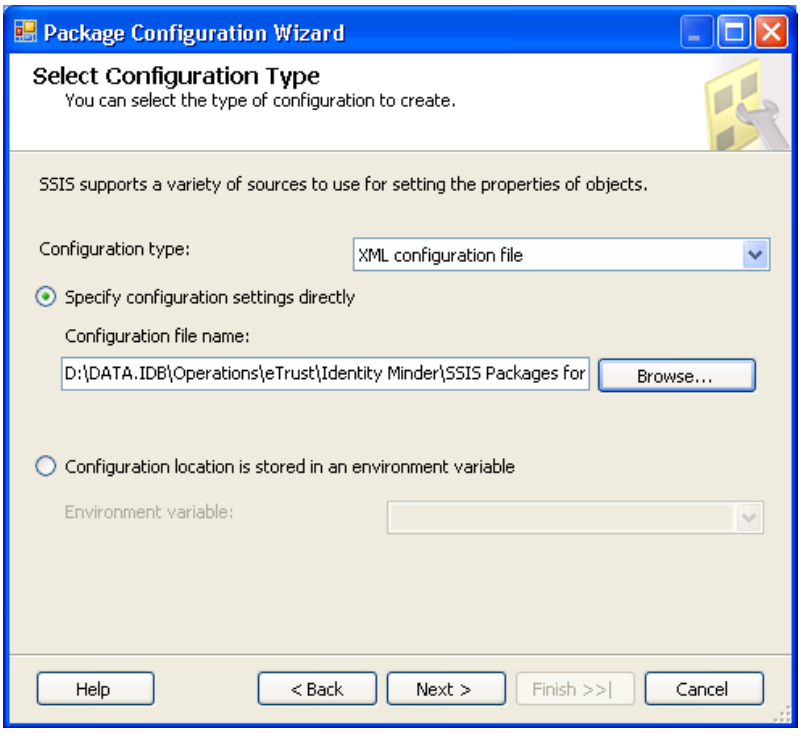
i. Haga clic en examinar…



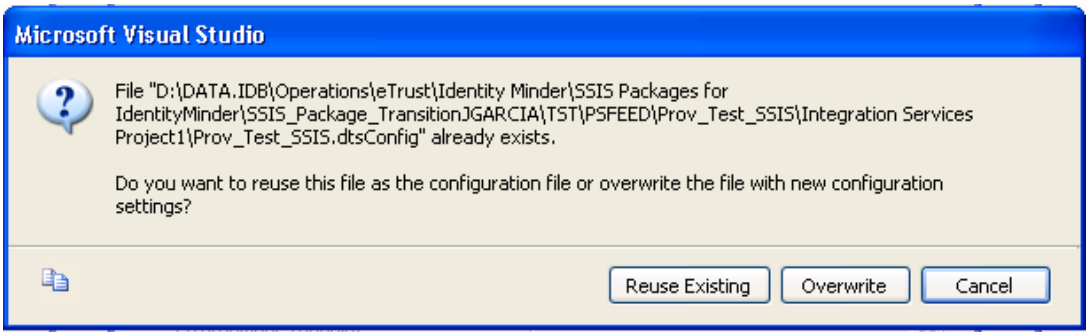
10. Vaya a la ubicación donde guradó .dtsConfig seleccionelo y haga clic en guardar



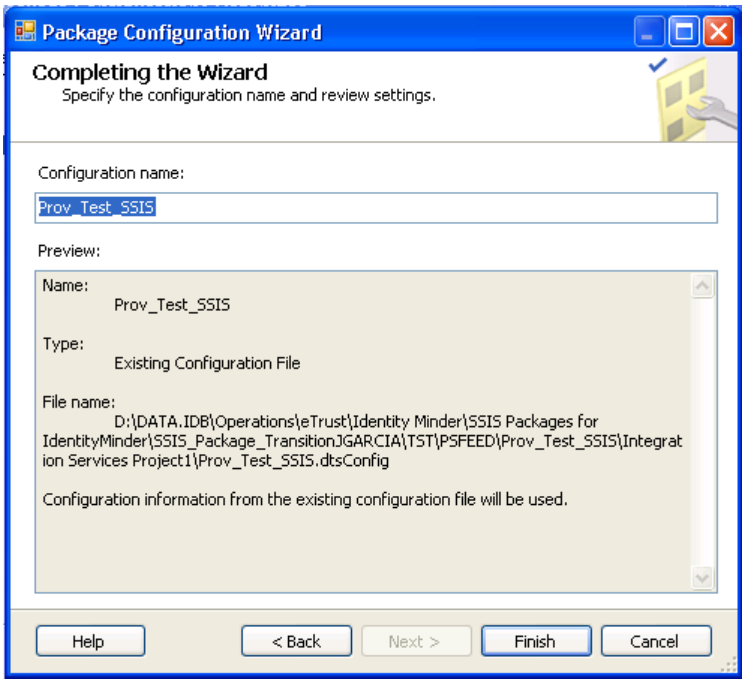
11. El archivo de nombre de configuración sera remplazado haga clic en siguiente>



12. Elija la opción de reutilizacion existente en el simbolo siguiente

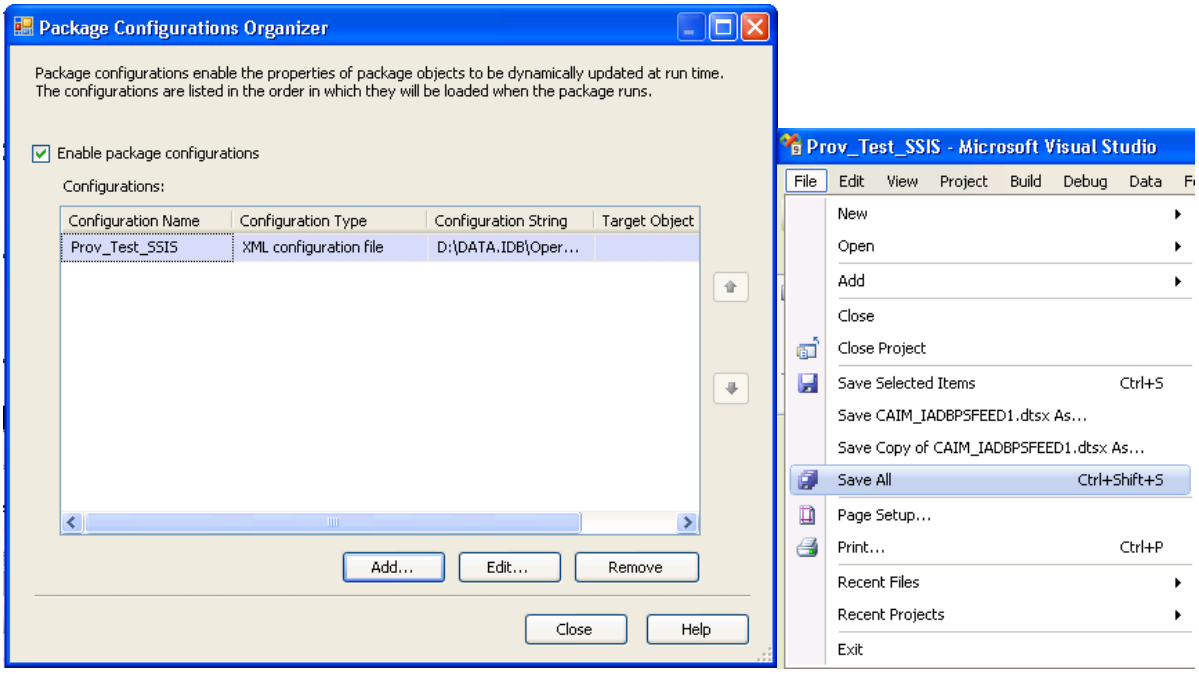


13. Introduzca un nombre para la configuración y haga clic en finalizar

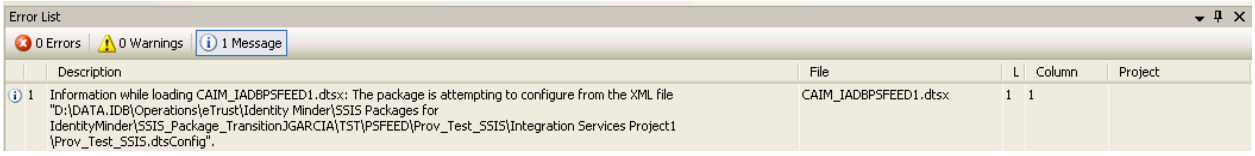


14. El archive de configuración estará disponible, haga clic en cerrar y salir al menu principal archive y guardar todo.

291



15. Abra de Nuevo el paquete, solo debe mostrar un mensaje que indica desde donde el paquete esta intentando configurarlo



4) Resumen

Usuario Global es una entidad , que tiene la lista de los diferentes objetos de cuenta . Todos los usuarios existentes en los dominios de AD se crearán como usuarios globales y otros sistemas de destino se correlacionaron basado en un atributo de correlación. A continuación se muestra un breve resumen de cómo integramos PeopleSoft HR con Identidad Minder y procesos en torno a la misma .

El logig que generan los siguientes eventos se encuentra en los procedimientos almacenados que se encuentran dentro de este documento en la página 22 - Procedimientos almacenados

BID Nuevo Proceso de Creación del usuario a través del administrador

1) Nueva entrada en PSFEED decir nuevo usuario con un EmployeeID y no los registros anteriores se han encontrado para ese usuario.

2) El usuario se agregará al nuevo archivo csv usuario con todos los ámbitos comprendidos en el extracto. Este archivo csv se archiva diariamente. Hay nuevos archivos de salida de usuario separadas para Personal y No Personal como se mencionó en la sección anterior.

3) Este será un aporte a la utilidad por lotes Identidad Minder

4) El usuario se creará como una identidad global

5) Sobre la base de la Org / Unidad al usuario se le asignará el papel (con múltiples políticas)

a. Política de Intercambio

b. Política de AD

6) Esto creará la cuenta de usuario en los sistemas de destino.

7) La contraseña de las cuentas de AD se establece en un complejo estándar ya que el técnico de instalación solicitará para restablecer a la hora de la orden de trabajo.

8) El proceso actual se sumará a los usuarios en los almacenes de datos de correo respectivo en base a la asignación definida por el BID. Buzones sólo serán creados para los usuarios que tienen

la bandera EmailAccount ajustado a "Y" en el archivo de la alimentación Peoplesoft.

9) El proceso actual se sumará a los usuarios en la siguiente estructura:

1) BID - OU: Temporal sin restricciones

a. BID - EXD - OU: Los usuarios EXD

2) REG - OU: Para aprobaciónFIN – OU FIN Users

a. Junto con la creación del usuario en la anterior unidad organizativa, administradores FIN serán notificados de la creación de usuarios a través de un papel UPO enviado por correo a las siguientes personas - ayuda FIN, cc: Dryan; CIRAP

2) Los usuarios de la CII serán creados por los administradores de dominio de la CII y la integración de recursos humanos con eTrust se ignorarlos. Estos usuarios serán creados como usuarios globales durante el correlato noche explorar.

3) Los usuarios COF: Los usuarios de COF se crearán en HQ COF dentro del dominio REG de acuerdo con las políticas y los roles asociados (se agregarán funciones en la tabla de SQL donde se define la asignación entre Org / unidad y el papel). Esto se replica en los controladores de dominio locales COF cada cuatro horas.

Estas especificaciones se definen en las políticas de publicidad y de correo para cada dominio, respectivamente, sobre la base de los requisitos del BID recopilación de documentos.

1) Los Administradores de AD y luego se trasladarán a los usuarios a la respectiva unidad organizativa de. (sólo para el BID y REG.)

2) La utilidad noche explorar-correlato se sincronizarán los cambios realizados en el sistema de destino de nuevo a eTrust administración

GU atributo AD Cuenta Atributo

Nombre

Apellido Nombre complete Mostrar nombre

Departamento Departamento

Customfield01

Subcadena carga útil (Offset 20 , longitud 6)

1) Los nuevos archivos de usuario se archivarán en el servidor diaria

2) El proceso de generación de ID de usuario será el siguiente:

a. La lista de los usuarios globales forman parte de todos los usuarios dentro de la organización (personal / Constultants etc) que figura en los Sistemas de Active Directory.

b. La lógica se comprueba antes de crear el usuario en la administración, a través de un procedimiento almacenado que es ejecutado con el paquete SSIS.

c. Los nombres de usuario globales se crean en el formato y el siguiente orden basado en la existencia de duplicados

Ejemplo: Nombre completo Peter B. Rabbit

1. FirstNameLastNameInitial (peterr)

2. FirstInitialLastName (PRABBIT)

3. FirstInitialMiddleInitialLastname (PBRABBIT)

4. FirstnameLastnameInitial (2) (Peterra)

5. FirstnameLastNameInitial (3) (PETERRAB)

6. Excepción - El registro se genera con los registros de excepción y SQA sería mirar el archivo username_exception.csv (HQPAPROVN \ D: \ psfeed \ output \ Excepciones)

3) Todos los usuarios del PSFEED con un tipo de usuario no igual al de staff son considerados como no correspondientes al personal y se procesan por separado. Nuevos Usuarios, Usuarios recontratados, Terminaciones, actualizaciones GU y transferencias son capturados por personal NO

población también y van a estar en el directorio HQPAPROVN \ D: \ psfeed \ output \ NONSTAFF

4) Los campos que se utilizan para el control y la actualización del psfeed son:

a. Nombre del jefe inmediato se añadirá a la Workflow aprobador

b. Número de empleado del jefe inmediato se añadirá a la Campo personalizado 02

c. ID de empleado se añadirá al Campo personalizado 01

d. ID de departamento se añadirá al campo Departamento

e. Tipo de usuario: El personal será añadido a un campo personalizado 05

f. ID viejo se añadirá a la Campo personalizado 03

g. Antiguo título se añadirá al campo personalizado 04

h. Comentarios del usuario recontratado se añadirán al Campo custom 06

5) Todo el proceso de creación de cuenta a través de Identidad Minder sería seguida por una notificación por correo electrónico al BID / FIN / REG - Administradores aviso , su asistencia y cc . El coordinador de instalación y el grupo Correo .

BID Administradores: servicio de asistencia de la ITF , EMAILGROUP cc . Maryjaneo , Siobhanb , Robertab

REG Administradores: ITCHelpdesk

REG COF Administradores: CXXTECHSUP para cada oficina en el país .

IADB Proceso de terminación a través del administrador.

1) Campo de estado es una indicación del estado de los usuarios dentro de BID

2) Tan pronto como el estado de un usuario cambia de 1 " activa" a 0 " Inactivo ", basada en la identificación de empleado la persona se termina

3) La bandera suspendido en Identidad Minder suspenderá todas las cuentas de los usuarios , junto con la identidad de usuario global

a. Este estado es un cambio en la identidad Minder que se puede convertir de nuevo a activo en caso de emergencia y todas las cuentas de usuarios se activará

4) Las fechas de finalización del contrato de los usuarios en el PSFEED se actualizarán en la identidad del usuario Global

a. Un trabajo por lotes se llevará a cabo todas las noches para comprobar la fecha de los usuarios finales y de acuerdo con que los usuarios suspendidos bandera se establecerá

b . Esto dará lugar a la suspensión de todas las cuentas de usuarios asociados .

5) Un correo electrónico será enviado a la SQAinfosec en un evento de una terminación

6) Un proceso BID necesita volver a certificar los roles para el usuario.

Proceso del banco IADB para volver a contratar a través del administrador IM

1) Campo de estado es una indicación del estado de los usuarios dentro de IADB

2) Tan pronto como el estado de un usuario cambia de 0 " Inactivo " a 1 " activo" en base en el número de empleado la persona es re- contratado

3) La bandera de activación en Identidad Minder se activará todas las cuentas de los usuarios , junto con la identidad de usuario global

a. Este estado es un interruptor en eTrust de administración que se puede convertir de nuevo a suspensión en caso de emergencia y todas las cuentas de usuarios se suspenderán

4) Un proceso BID necesita haber recertificado los papeles y representa para el usuario.

5) Un correo electrónico será enviado a la siguiente en un evento de una recontratación

IDB Administrators: ITF helpdesk, EMAILGROUP

REG Administrators: ITCHelpdesk

REG COF Administrators: CXXTECHSUP for each country office.

IADB Proceso de tranferencia a través del administrador IM

1) El cambio en el ID de departamento: Org / Unidad es una indicación de una transferencia de un usuario.

2) Tan pronto como el Org / Unidad ha cambiado para un Rol aa usuario transferencia se asocia con ese usuario, que envía un e-mail a un grupo de personas que notifican que un usuario ha sido transferido y administradores que tomar medidas dentro de la meta sistemas

3) Los administradores harán los cambios necesarios en los sistemas de destino y explorar todas las noches proceso correlato de Identidad Minder se actualizará ese objeto en el directorio

4) El personal en excedencia se considera como transferidos de una unidad organizativa a los específicos SRE / LVE, SRE / SPC, SRE / SPA y estos registros serán manejados de manera similar. El campo de estado también se procesará en consecuencia. Así, si el estado es recibido como inactiva, entonces el usuario global se desactivará con todas las cuentas asociadas.

5) El correo de notificación contendrá los siguientes campos

a. Nombre de usuario

b. Global Nombre de usuario

c. Apellido

d. Nombre de pila

e. ID No.

f. Unidad Organizacional Anterior

g. Nueva Unidad Organizacional

h. user type

6) de transferencia para el internacional al local

a. PS alimentación tendrá un cambio en la Org / Unidad de dicha transferencia

b. Usuario vendría en la alimentación como 2 entradas una de ellas con un status: 0 "Inactivo" y anterior Org / Unidad y el otro con el estado: 1 "activa" y la nueva Org / Unidad

c. La entrada de usuario con el estado 1 "activa" será considerado y el Usuario Global se actualizará con los nuevos datos.

1) The UPO e-mail will be sent to the following list of people informing about the transfer:

SQAInfosec

IDB Administrators: ITF helpdesk, EMAILGROUP

REG Administrators: ITCHelpdesk

REG COF Administrators: CXXTECHSUP for each country office.

eTDN: eTUPOAccountName=testupo4,eTUPOAccountContainerName=Accounts,eTUPODirectoryName=TRANSFER,eTNamespaceName=Universal Provisioning,dc=IADB,dc=etasa

eTName: testupo4

eTUPOUserData: Last Name = upo4

First Name = test4

ID No. = 12345

Previous Org Unti = Old

New Org Unit = New

Old Title = Jr Accounttant (Old)

New Title = Jr Accountant (New)

eTUPOGlobalUserName: testupo4

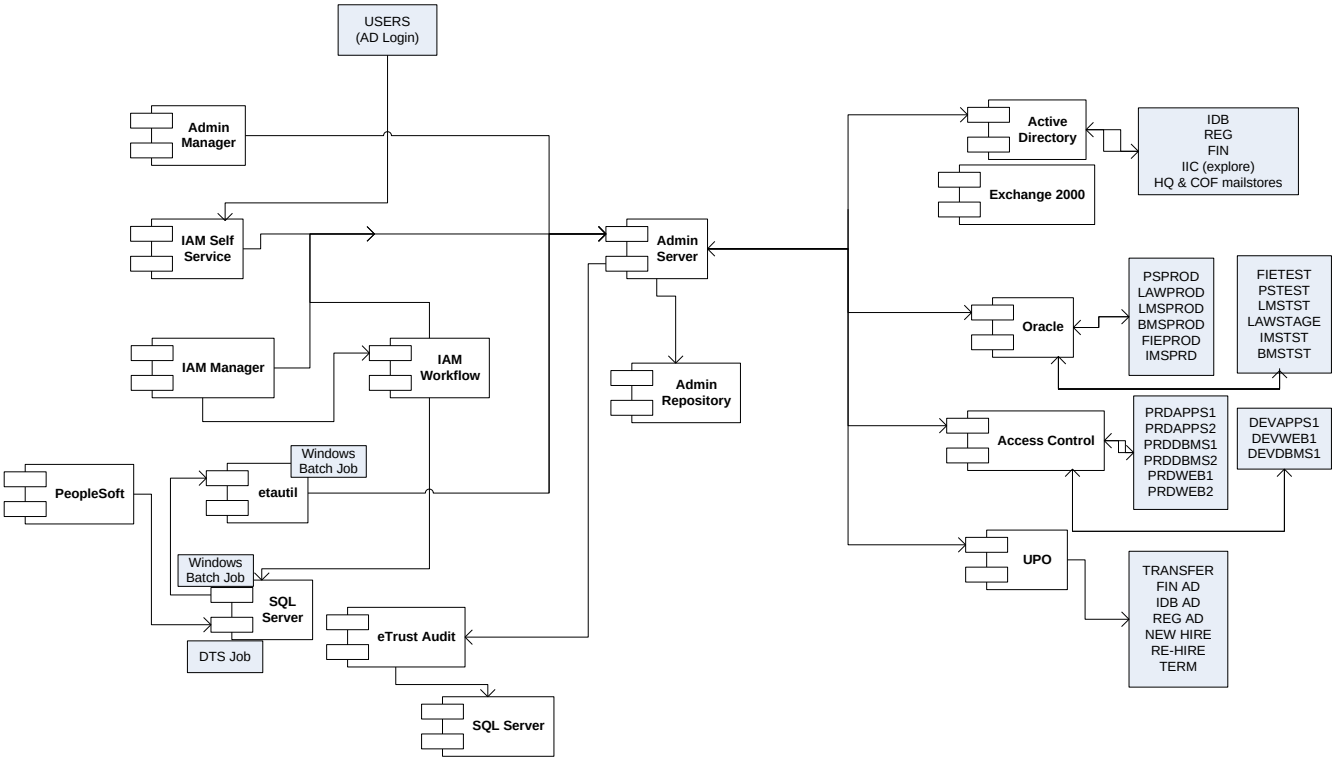
eTSuspended: 0

eTAccountStatus: A

eTUPOAccountName: testupo4

createTimestamp: 20060301215327Z

5) Diagrama de integración



El diagrama anterior enumera los diferentes componentes de la solución de aprovisionamiento de usuarios en su sitio.

SQL Server - paquete SSIS y procedimientos almacenados para dar una entrada al ETAUTIL

Empleos por lotes - Ejecutar " etautil " comandos para la entrada de eTrust Admin para iniciar el aprovisionamiento / actividad de aprovisionamiento

Los sistemas que serán gestionados por la producción de eTrust Admin:

1) Directorios de prueba

2) Directorios de producción

1. SOLUCIONES DE IMPACTO Y PROCESO DE FALLAS

Nightly sincronización Proceso Fallo:

Impacto:

1) Sin impacto será el sistema de destino y eTrust administración

2) El proceso de explorar correlato o el trabajo por lotes cuando se ejecuta manualmente , todas las actualizaciones se harán en eTrust Admin (Ver instrucciones de ejecución manuales anteriores)

Resolución / Notificación :

1) Si el fallo proceso de sincronización de todas las noches se debe a que el trabajo por lotes no se ha ejecutado a continuación ControlM al BID alertará a la autoridad respectiva BID - Un trabajo Control-M tiene que ser creado .

PS fallo de alimentación Extracto de PeopleSoft

Impacto:

1) Nuevo proceso de usuarios / Usuarios Terminados / Usuarios recontratados / Usuarios transferidos no funcionará para ese día. El archivo creado será un archivo vacío , ya no habrá delta.

Resolución / Notificación :

1) Tan pronto como el nuevo alimento que se haya recibido todos los usuarios a partir del día de la falla hasta la fecha se manejará como normal y procesos tendrá en cuenta los 4 eventos (Nueva usuarios / Usuarios Terminados / Usuarios recontratados / Usuarios transferidas)

302

ETAUTILITY failure

Impacto:

1) Nuevo proceso de usuarios / Usuarios Terminados / Usuarios recontratados / Usuarios transferidos no funcionará para ese día de forma automática

Resolución / Notificación:

1) Si el fallo de proceso por lotes etautil noche se debe a que el trabajo por lotes no se ha ejecutado a continuación ControlM al BID alertará a la autoridad respectiva BID

2) necesitarán Los archivos comprimidos para ser colocado en la carpeta raíz y necesitarán el proceso por lotes que se ejecute de forma manual, entrada doble no se crean y se crearán sólo las entradas que faltan

3) Los archivos de almacenamiento se crean antes del proceso de administración es decir etautil se ejecuta. Así que podemos ejecutar el archivo por lotes manualmente para tener un proceso semi-automático.

Fracaso DTS Trabajo

Impacto:

1) Nuevo proceso de usuarios / Usuarios Terminados / Usuarios recontratados / Usuarios transferidos no funcionará para ese día

Resolución / Notificación:

1) Si el fallo de proceso por lotes DTS noche se debe a que el trabajo por lotes no se ha

ejecutado a continuación Programador SQL mostrará un error para el DTS Trabajo.

2) Para volver a ejecutar el trabajo DTS para un día en particular, vacía los existing_users y mesa nightly_feed y la carga tanto de las tablas del archivo existing_users.csv último de la carpeta existing_users_bkup copia de seguridad.

304

6) Especificaciones

Datos de entrada

prov_file.txt –

Este es el esquema de un record de usuario

UserName|FullName|FirstName|LastName|MiddleName|employeeID|EnableDt|DisableDt|DeptId|Title|Company|Phone|PrimaryMail|ManagerId|ManagerUserName|Status|PreferredFirstName|Location|DeptDescr|EmpldRcd|StreetAddress|City|State|PostalCode|Country|UserType|ADAccount|EmailAccount|AlternateEmplid

Ejemplo de un record de usuario:

SOLVEIR|Rasmussen,Solvei|Solvei|Rasmussen||777500|03/01/2016|03/01/2020|ITE/ITE|Smoke Test User|IDB|202/623-1277|| ||1| |HQ|InterAmerican Development Bank| 1| | | | |Staff|Y|Y|

Todos los records de los usuarios se encuentran en el archivo de texto Prov_file.

a. CASO I

b. Nuevo empleados:

Tipo de usuarios –

a) Empleados a tiempo completo indicado por el personal

b) Consultores indican con Contractual , Contratista y adscrito

Pasos para personal/no personal

- Cuenta de AD y cuenta de correo electrónico se crearán sobre la base de las banderas ADAccount y EmailAccount .

Entrada:

MARTAAB|Abello,Marta Isabel|Marta|Abello|Isabel|105758|04/30/2005||FIN/APR|Pr Accountant II|IDB|202/623-3542|martaab@iadb.org|105407|ALBERTOSU|1| |HQ|Acctg Policy/Reports Section|0|57 Calabash Court |Rockville|MD|20850|USA|Staff|Y|Y|28935

UserName|FullName|FirstName|LastName|MiddleName|employeeID|EnableDt|DisableDt|Dept Id|Title|Company|Phone|PrimaryMail|ManagerId|ManagerUserName|Status|PreferredFirstName|Loca tion|DeptDescr|EmpldRcd|StreetAddress|City|State|PostalCode|Country|UserType|ADAccount|Email Account|AlternateEmplid

- Crear Nuevo usuario Global

Actualizar campos :

Global usuario - insumos alimenticios

Nombre de usuario - Generar nombre de usuario utilizando la lógica aprobada

AccountName - Igual que el nombre de usuario global

FullName - NombreCompleto

Nombre

Apellidos - Apellidos

MiddleName - MiddleName

Empresa - Empresa

Teléfono - Teléfono

Habilitar Fecha - EnableDt

Fecha Desactivar - DisableDt

Dept ID - DeptId

- Asignar rol para el usuario

Dar específico que Papel AD dominio basado en el departamento

Cuenta antidumping de base

Cuenta Bolsa básica

- Usuario sincronización con Papel

Crear Cuenta antidumping de base

Crear una cuenta de Exchange Básica

- Gerente Actualizar Usuarios

- Actualizar Usuarios Employee ID - Custom Field01

- Identificación Gestores de actualización de usuarios Empleado - Custom Field02

- Actualización Definido por el usuario - field05 personalizada

- Actualización Field07 personalizada con comentario " No Mail Box requerida" si ADAccount = " Y" y EmailAccount = " N "

Eg: ETA FILE

add "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

```
  eTGlobalUser GlobalUserName="donagl1"
  eTFirstName="GLORIA"
  eTLastName="DONAHUE"
  eTFullName="DONAHUE, GLORIA"
  eTUserid="donagl1"
  eTTitle="POLYSOMNOGRAPHER, REG"
  eTEnableDate="0000106073"
  eTDepartment="Sleep Lab"
  eTLocation="Virginia Baptist Hospital"
  eTStreetAddress="Virginia Baptist Hospital/Sleep Lab"
  eTDescription="ETRUST created on Feb 13 2006 10:00PM"
  eTCustomField01="7808"
  eTCustomField02="GLORIA"
  eTCustomField03="02-14-2006"
  eTSelfAdminPermitted="1"
  eTPropagatePassword="1"
  eTwfSecurity="AS"
  eTPassword="GDo0935";
add "eTRoleContainerName=Roles,eTNamespaceName=CommonObjects"
  etRole eTRoleName="Basic User"
  in  "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"
  eTGlobalUser eTGlobalUserName="donagl1";
```

update "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

eTGlobalUser GlobalUserName="donagl1" to

eTSyncUsers="1";

update "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

eTGlobalUser GlobalUserName="donagl1" to

eTSuspended="1"

eTSyncAccounts="1";

update "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

eTGlobalUser GlobalUserName="donagl1" to

eTSuspended="0";

update "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

eTGlobalUser GlobalUserName="donagl1" to

eTwfManager="eTGlobalUserName=thacir1,eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects,dc=IADB";

c. CASO II

d. Usuarios predeterminados

Cambie la Condición de Usuario Global de un objeto en el alimento cuyo estado ha cambiado de 1 a 0

309

- Banderas Fix jgarcia 05.13 / 2013-- Si el usuario no es personal , no de la CII , cambió banderas AD de Y a N, fue activo en el ayer Prov_file y tiene un nombre de usuario , entonces se gestionará como una terminación .

- Eg: ETA FILE

update "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

eTGlobalUser GlobalUserName="blanma1" to

eTSuspended="1"

eTSyncAccounts="1";

11.5 CASO III

11.6 USUARIOS recontratados

- Cambie la Condición de Usuario Global de un objeto en el alimento cuyo estado ha cambiado de 0 a 1

- Banderas Fix jgarcia 05/13/2013 - Si el usuario no es de la CII , cambiado banderas AD de n ay, está activo y tiene un nombre de usuario , entonces se gestionará como una recontratación

Ej : ETA ARCHIVO

update "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

eTGlobalUser GlobalUserName="blanma1" to

eTSuspended="0"

eTSyncAccounts="1";

11.5 CASO IV

11.6 TRANSFERENCIAS

Input:

MARTAAB|Abello,MartaIsabel|Marta|Abello|Isabel|105758|04/30/2005||FIN/APR|Pr Accountant II|IDB|202/623-3542|martaab@iadb.org|105407|ALBERTOSU|1||HQ|AcctgPolicy/Reports Section|0|57 Calabash Court |Rockville|MD|20850|USA|Contractual

UserName|FullName|FirstName|LastName|MiddleName|employeeID|EnableDt|DisableDt|Dept Id|Title|Company|Phone|PrimaryMail|ManagerId|ManagerUserName|Status|PreferredFirstName|Location|DeptDescr|EmpldRcd|StreetAddress|City|State|PostalCode|Country|UserType

- Tan pronto como el ID de departamento se ha cambiado en la alimentación , la indicación de una transferencia de un usuario

- Asignar UPO Rol de usuario , que enviará una notificación por correo electrónico con respecto a la transferencia, y por lo tanto los administradores van a hacer la transferencia

- Banderas Fix jgarcia 05.13 / 2013-- Cuando el usuario es no personal y tiene AD Bandera Y o cuando el usuario no es personal y tiene nombre de usuario

Eg: ETA FILE

add "eTRoleContainerName=Roles,eTNamespaceName=CommonObjects"

etRole eTRoleName="UPO Transfer Role"

in "eTGlobalUserContainerName=Global Users,eTNamespaceName=CommonObjects"

eTGlobalUser eTGlobalUserName="donagl1";

7) Base de datos:

1. Produccion

IDBPRDA1\IDBPRDA1INST1: ETAPSDBPRD (Base de datos)

IDBPRDB2\IDBPRDB2INST2: IADBPSFEED1 (DTS Paquete)

a. Test

IDBTRDA1\IDBTRDA1INST1: ETAPSDBTST (Base de datos)

IDBTRDB2\IDBTRDB2INST2: IADBPSFEED1 (DTS Paquete)

b. Dev

HQTD01

ETAPSDBTST (Base de datos)

IADBPSFEED1 (DTS Paquete)

13. Los procedimientos almacenados :

sp_validate_psfeed : Este procedimiento compara los datos en nightly_feed_new con nightly_feed y si nightly_feed_new tiene registros de menos de lo que se espera (registros en

312

nightly_feed - 5) y luego se inserta un registro de mensaje de error en la tabla failsafe_errormessage que indican que la alimentación entrante tiene menor número de registros de lo esperado . Si nightly_feed_new tiene el número esperado de registros entonces se copian en el nightly_feed y luego procesado

sp_create_userid : Este procedimiento tiene la lógica para eliminar los registros duplicados para el personal y no personal sobre la base de la identificación de empleado . La entrada a este procedimiento almacenado es de mesa nightly_feed y la salida es a la mesa nightly_feed_unique . (Este procedimiento almacenado anterior tenía lógica creación nombre de usuario, el cual fue más tarde, se trasladó a sp_nightly_feed_in .)

sp_nightly_feed_in : Este procedimiento procesa los datos de entrada de nightly_feed_unique . sp_nightly_feed_in tiene la lógica de construir en identificar nuevos usuarios , Terminaciones , Traslados , recontrataciones y Usuario Global actualizaciones . sp_nightly_feed_in también tiene lógica para crear un nombre de usuario único para los nuevos usuarios . Antes de crear nuevos usuarios hay un control de identidad de los empleados contra la mesa Global_Users para asegurarse de que el usuario no existen ya en el año . New_Transfer_Roles es otra tabla de entrada a sp_nightly_feed_in . Esta tabla tiene las unidades organizativas y las funciones relacionadas. Los datos de salida de sp_nightly_feed_in va a las tablas a continuación se enumeran

sp_fail_safe : Este procedimiento tiene es para a prueba de fallos . Comprueba si el número de registros en Nueva usuario , Terminado usuario , recontratados usuario y Transferido Usuario cabo puso archivos tanto para el personal y no personal , y si el recuento es mayor que 100 , se mueve los

313

datos a los " faildump " tablas . No hay archivos se generarán en esa fecha para el nuevo usuario , Terminado usuario , recontratados usuario y eventos de usuario transferidos . Un mensaje de error se escribirá en failsafe_errormessage mesa. Por favor, consulte el documento de configuración Proceso por lotes para la lista detallada de las tablas .

8) DTS PAQUETE:

Archivo de texto (Source) - **\\HQPAPROVN\psfeed$\input\prov_file.txt**

HQPAPROVN\D:\psfeed\output\STAFF

new_users_role.csv

rehired_users_role.csv

terminated_users.csv

transferred_users.csv

updated_mgrs.csv

HQPAPROVN\D:\psfeed\output\NONSTAFF

new_users_role_nonstaff.csv

rehired_users_role_nonstaff.csv

terminated_users_nonstaff.csv

transferred_users_nonstaff.csv

updated_mgrs_nonstaff.csv

HQPAPROVN\D:\psfeed\output\Exceptions

existing_users.csv

username_exception.csv

failsafe_errormessage.csv

new_users_role_faildump.csv

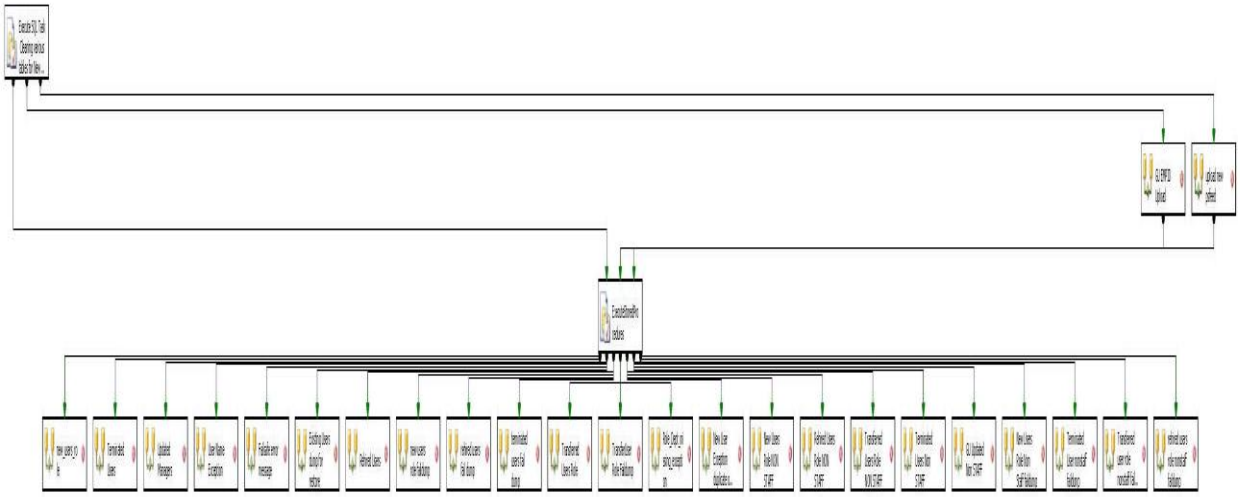
rehired_users_faildump.csv

terminated_users_faildump.csv

transferred_users_faildump.csv

New_users_exception.csv

Role_Dept_Missing_Exception.csv



14. EJECUTABLES PARA PROCESAR CSV - LOTE DE PROCESAMIENTO DE ARCHIVOS

Los archivos de C # se enumeran a continuación para todos los 5 anteriores condiciones

1) Nuevos Usuarios

2) Los usuarios terminados

3) Los usuarios transferidas

4) Los usuarios recontratados

5) cambios GU

Los códigos fuente de estos programas se encuentran en:

\\ HQPAPROVN \ D: \ etascripts \ Programas \ SourceCode_latest

Las últimas ejecutables se encuentran en

\\ HQPAPROVN \ D: \ etascripts \ Programas \ executables_latest

316

Tabla 51 - Definición de Terminos

Termino	Definicion
Tipos de Endpoint (Namespaces)	Un tipo de endpoint es un tipo específico de aplicación que será administrado por el sistema, como Microsoft Exchange u Oracle que son administrados por Identity Minder. Anteriormente, un endpoint type se conocía como namespace.
Endpoint (Directorios)	Un endpoint es una instalación específica de un Endpoint type, como Microsoft Exchange instalado en el servidor. Anteriormente, un Endpoint se conocía como Directorio.
Ambiente	Un ambiente hace referencia a todos los servidores y los sistemas de apoyo - redes, firewalls y otro hardware y aplicaciones utilizadas para albergar soluciones. Los ambientes se pueden construir en máquinas físicas o virtuales y se requerirán diferentes ambientes para las diferentes etapas de una solución de entrega, por ejemplo: desarrollo, prueba, puesta en marcha y producción
Plantillas Cuenta (Políticas de aprovisionamiento)	Puede crear plantillas de cuentas en el Administrador de aprovisionamiento(Provisioning Manager). Estas plantillas proporcionan la base para las cuentas en un endpoint type específico. Anteriormente, una plantilla de cuenta se conocía como política de aprovisionamiento
Servidores de conectores (Agente plug-ins)	El servidor de aprovisionamiento se comunica con el sistemas de punto final a través de servidores de conectores y conectores. Existen dos tipos de conectores, C ++ servidor de conector (CCS) y el servidor de conector de Java (JCS)
Componente	Se refiere a una instancia de software instalable , incluyendo los productos de CA que pueden incluir ejecutable (s) y / o datos.
Parametros	Un parametro es una cantidad o el valor que define ciertas caracteristicas de sistemas o funcionamientos. Los parametros son usados para personalizar un programa para requisitos o especificaciones a la solución de un cliente.

Termino	Definición
AD	Microsoft Active Directory
Actores	Los roles de usuario o sistemas que interactúan directamente con la solución.
Disponibilidad	La copia de seguridad / restauración y las características de respaldo de la Aplicación.
CA Identity Manager	CA Identity Manager es un producto de gestión administrativa que proporciona servicios automatizados de gestion de identidad para la creación, modificación y eliminación eventual de cuentas y derechos sobre la base de las relaciones de los usuarios. Gestiona el acceso y los derechos de toda una gama de sistemas empresariales, desde mainframes hasta aplicaciones Web.

Termino	Definición
Componentes	Una instancia de sofware instalable que puede incluir un ejecutable o base de datos. La Solucion de modelo arquitectonico puede listar el software de CA, para entornos personalizados de clientes o proyectos, o bien desarrolladores de componentes si alguno es requerido para dicha solución.
C/R	Reto / Respuesta
DTS	Data transformation (MS SQL 2008 specific)
Ambiente	Un ambiente hace referencia a todos los servidores y los sistemas de apoyo - redes , firewalls y otro hardware y aplicaciones utilizadas para albergar soluciones. Los ambientes se pueden construir en máquinas físicas o virtuales y se requerirán diferentes ambientes para las diferentes etapas de una solución de entrega, por ejemplo: desarrollo, prueba, puesta en marcha y producción
EULA	End-User License Agreement
Failover	Failover se refiere a la habilidad de recuperar un componente fallido en tiempo real.
GSE	CA Equipo Global de soluciones de ingenieria de servicios
IAM	Identity and Access Management (Administración de Identidad y acceso)
ICC	Centro de informacion al cliente (Helpdesk)
IM	CA Identity Manager
IT/Manejo de Negocios	La acción inicial que impulsa la necesidad de una solución
LOB	Linea de Negocios
OOTB	Fuera de caja
Arquitectura Fisica	La estructura que define cómo se implementan los componentes del producto para lograr una solución.
QoS	Calidad del servicio
Confiabilidad	Características de buen funcionamiento y rendimiento de la solución.
Requerimientos	Parte 1 (Secciones 1 y 2) del Diseño Detallado (SAS) o de la especificación de requisitos de la solución.
ROI	Retorno de la Inversión
SAN	Red de area de almacenamiento

318

Termino	Definición
SAO	Arquitectura de la solución general - un producto de trabajo entregado por el personal de CA para un cliente para ayudar a la producción de un diseño de soluciones de alto nivel. La SAO se utiliza para ayudar a los requisitos del cliente y resultados del proyecto , incluyendo las funciones, soluciones métricas y alcances. La SAO propone arquitectura, implementación, y validación enfocado en cómo los productos de CA pueden ayudar a mantener los resultados del proyecto. En caso de cualquier conflicto entre una Declaración de Proyecto de Trabajo y una SAO , la Declaración de Trabajo tiene prioridad sobre la SAO .
Utilidad	Una descripción de la administración y mantenimiento de la aplicación
Solución	La implementación propuesta de CA software para el entorno del cliente , que se detalla en este documento.
Calculadora de Soluciones	Una calculadora de Soluciones es una hoja de cálculo que cuando se completa con un Arquitecto , calculará las estimaciones de esfuerzo de trabajo para la implementación de CA Soluciones en el entorno de un cliente. Incluye disposiciones para aquellas circunstancias donde hay una buena SAO, una SAO incompleta o en el peor de los casos donde no hay SAO . La salida de un Calculadora dará la más precisa estimación de esfuerzo del proyecto posible, depende de la información disponible. Incluye cálculos de los parámetros, estimación de requerimientos para la personalización del cliente, además de horas requeridas para el equipo del proyecto.
Solución métrica	Medida cuantificable de los resultados del proyecto.
Prueba de solucion metrica	Prueba que ayuda a validar que una solución métrica se ha logrado.
Requisitos de solución	Uno de los resultados funcionales propuestos para la Solución
Solucion libro ejecutable	Detalles de enrutamiento de los procedimientos de mantenimiento, funciones administrativas clave, la seguridad y el control de la información de la Solución. También proporciona una guía de solución de problemas para los administradores y personal de operaciones .
TEWS	Ejecución de tareas de servicio Web
UPO	Provisioning conector universal (UPO) proporciona un mecanismo para Identity Manager para recurrir a programas externos especificados por el usuario cuando se reciben solicitudes del aprovisionamiento de usuarios.
Casos de uso	Objetivo funcional que un actor puede tener de la Solución. Cada Requisito de Solución tendrá uno o más casos de uso correspondientes .

Termino	Definición
Prueba de casos de uso	Una prueba que ayuda a validar que una meta de casos de uso se ha cumplido.

320

Apendice

CA Identity Manager Solution Integration Specification v1_3 – Cómo instalar la aplicación

321

1 Supuestos

El documento está escrito basado en el entendimiento de que el lector tendrá un buen conocimiento del sistema operativo y todas las aplicaciones de terceros que son requisitos previos para la configuración de la solución IdentityMinder .

El lector y administrador deben tener conocimiento de la configuración de los siguientes productos :

- Base de datos Microsoft SQL Server
- WebSphere Application Server
- Directorio de CA
- CA SiteMinder Política servidor
- IIS Web Server
- CA SiteMinder agente web
- CA Identity Manager
- Servidor IM Provisioning

En este manual se asume que una conjunto de políticas de SiteMinder existente está presente y todos los requisitos previos se han cumplido como se indica en la solución Especificaciones de Diseño.

Todos los valores de los campos que no requieren un parámetro designado específica conservarán sus valores por defecto.

Tabla 52 - Instalación Herramientas necesarias – Pre-requisitos

Nodo	Requisitos de configuración
Soporte de aplicación de servidor	Websphere servidor de aplicaciones 7.0 debe estar en ejecución antes de instalar CA Identity Manager.
Soporte de servidor aplicación J2SE for	JDK 1.6.0_22 o más actual
Base de dator	SQL servidor 2008 debe estar instalado

1.1 Entornos

Hardware – los nodos de hardware deben estar configurados con la memoria apropiada, procesadores y espacio en disco duro asi como sistema operativo.

Network – reglas de firewall , entradas DNS , arrendamientos DHCP , las direcciones IP asignadas y otros requisitos de configuración de red que lo completan

Tabla 53 - Componentes de soporte

Directorio Activo	Active Directory debe estar configurado para el uso de licencias
Base de datos	SQL Server 2008 Se debe de instalar el paquete de servidor más reciente
Soporte J2SE	CA Identity Manager requiereJDK 1.6.0_22 o más actual

a. Dependencias externas

Las siguientes dependencias externas deben estar en su lugar antes de la instalación de la solución puede empezar :

1.1.1 RDBMS base de datos

Una versión compatible de un RDBMS , SQL Server 2008 debe estar instalado y una base de datos debe ser creado para albergar los almacenes de datos necesarios para Identity Manager.

1.1.2 Servidor Web

Instale una versión de la base de IIS Server mediante el proceso de construcción estándar.

Java JDK/JRE

Instale los componentes JDK / JRE en las máquinas de Identity Manager y Provisioning Server compatibles.

Websphere Application Server

El WebSphere Application Server debe estar instalado y en ejecución de acuerdo con la configuración estándar.

2

Las instrucciones de aplicación previstos aquí están para ayudar al implementador y no son un sustituto de los manuales del producto . La aplicación creará un documento de compilación detallada que debe tener instrucciones de instalación paso a paso .

Requisitos Tecnicos

1. Obtener los nombres de todas las máquinas .

2. Administrador / Acceso de root en el servidor de mensajería instantánea y servidor de aprovisionamiento .

3. cuenta de administrador local es necesario para instalar los componentes de servidor de aprovisionamiento

4. Identity Manager requiere dos cuentas de usuario que son normalmente representa regulares , como sigue:

• Una cuenta que es utilizada por Identity Manager como el administrador del sistema de forma predeterminada (recomendado nombrarlo SuperAdmin o imadmin)

• Una cuenta que se utiliza como proxy para las tareas del pubis Auto Servicio (nombre recomendado es impublicuser)

• Una cuenta que se utiliza para la entrada de sincronización. Ningún usuario inicia sesión en esta cuenta de usuario , sino que se utiliza internamente por Identity Manager

(Nombre recomendado es inboundadmin)

2.1 Procedimiento de instalción

325

2.1.1 Instalación de JAVA

El JDK necesita ser instalado en todas las maquinas necesarias como y cuando sea necesario.

Los archivos descargados de http://java.sun.com/j2se/

- JDK

o Se puede encontrar en http://java.sun.com/j2se/ y luego buscar las versiones anteriores de descarga

o Usado por Directorio

o Nota: Todos los archivos de instalación se encuentran en servidores de prueba del BID en D: \ Archivos de instalación de software . Así que los archivos de instalación , incluyendo Java se pueden encontrar aquíFIPS key creation

FIPS es necesaria sólo para organizaciones federales. Al BID no estamos utilizando FIPS.

2.1.2 Instalar directorios en servidor de abastecimiento

En la máquina "CA Provisioning Server" , inicie sesión como "Administrador" para completar la instalación .

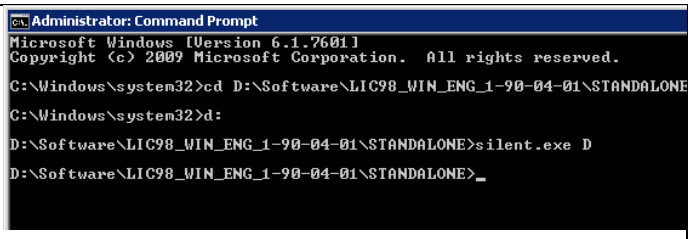
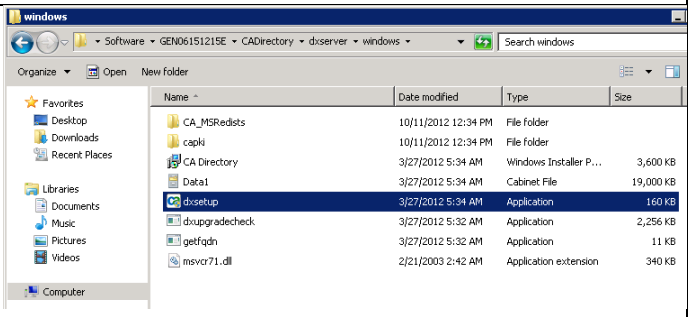
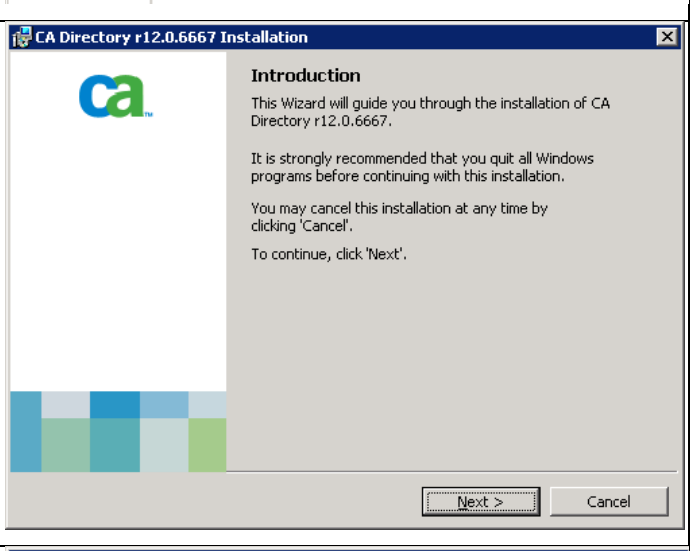
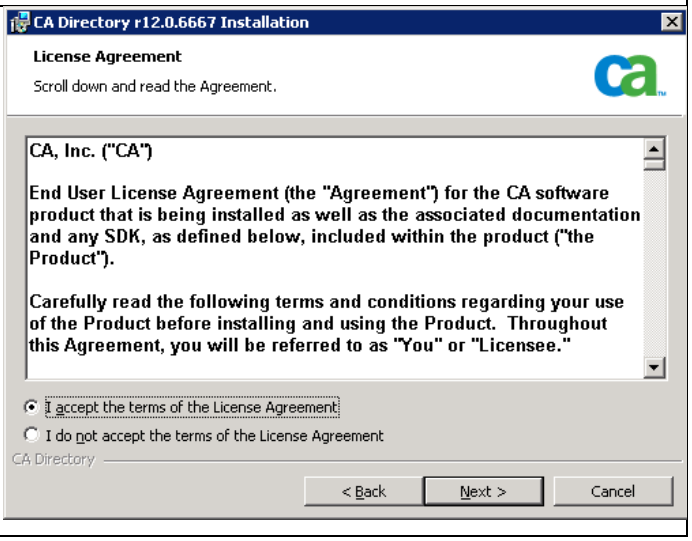
Requisitos de instalaciónn

- Asegúrese de que la versión necesaria del JDK en instalarse en la máquina y JAVA_HOME se establece acertadamente

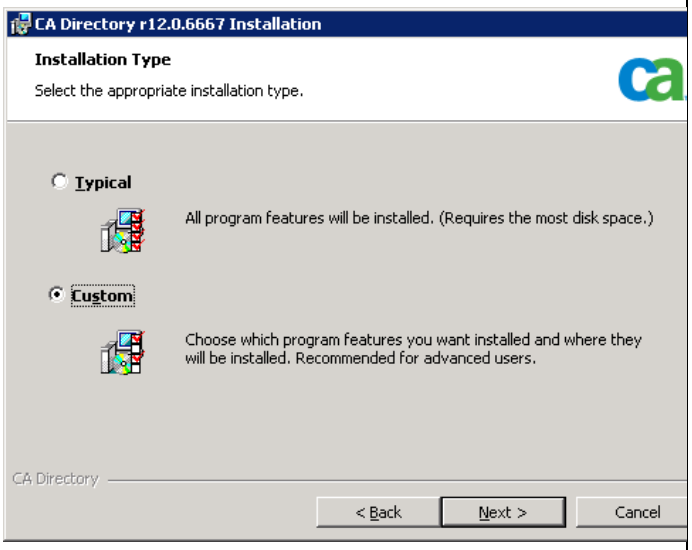
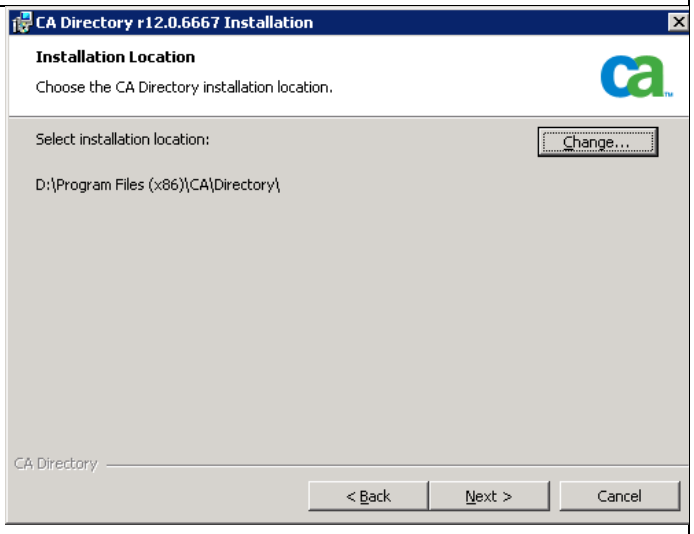
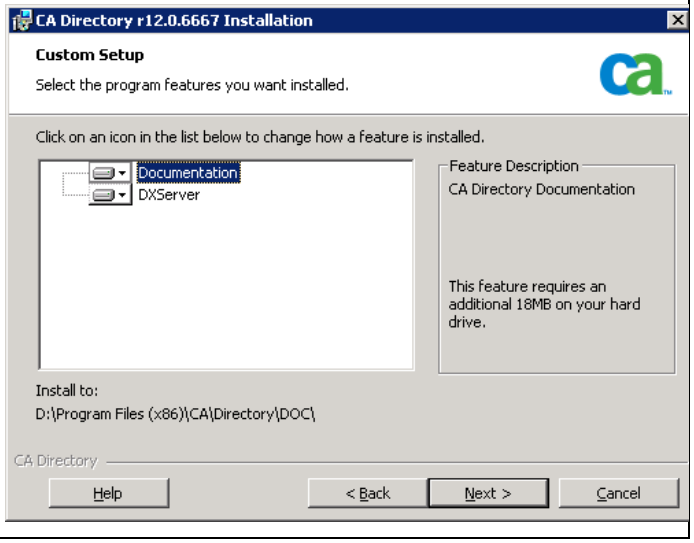
Nota : Instale de directorio de CA que se requiere en el equipo en el servidor de aprovisionamiento se instala como servidor de aprovisionamiento necesita un router local en el cuadro local.

Pasos para Instalación

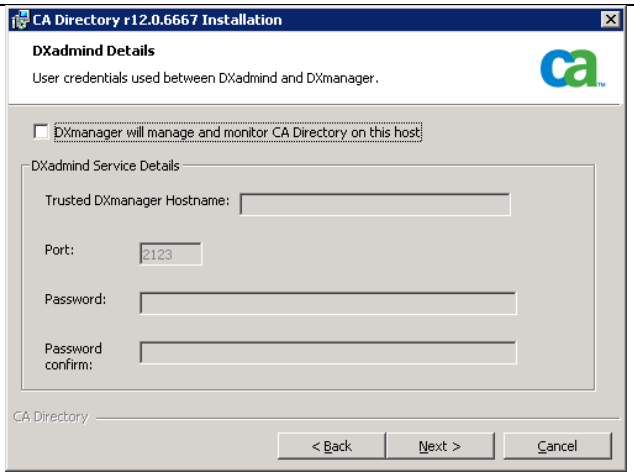
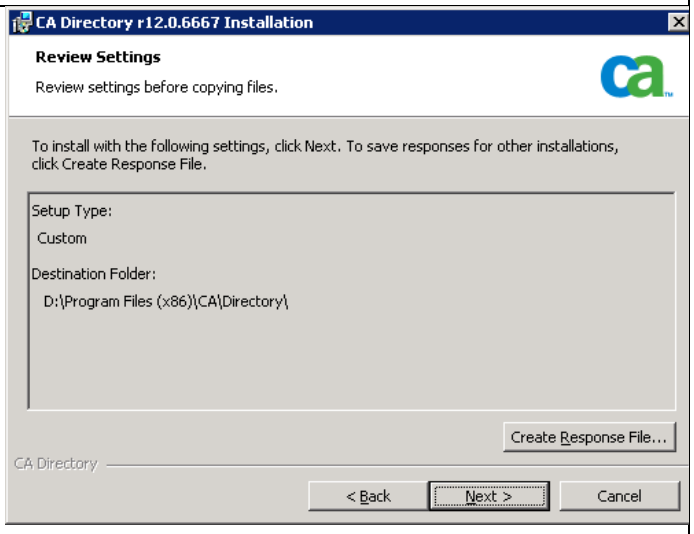
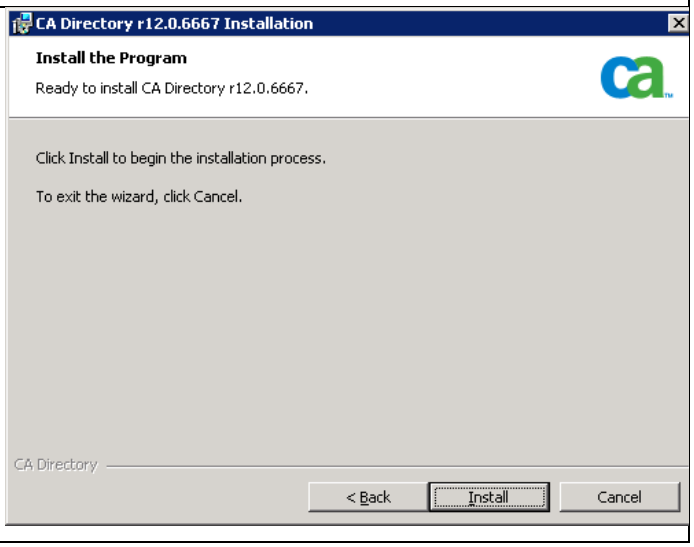
2.1.3 Instalar directorios en primarios

En el servidor de aprovisionamiento, desde un símbolo del sistema ventana de exploración a D: \ Sotware \ LIC98_WIN_ENG_1-90-04-01 \ INDEPENDIENTE (O el equivalente en donde se instalan los archivos de licencia directorio) ejecutar silent.exe D. D especifica la unidad en la que desea que se instale a	
Busque la configuración de Directorio en "D: \ Software \ GEN06151215E \ CADirectory \ dxserver \ windows " Ejecute el archivo ' dxsetup.exe ' como " Administrador" .	
Haga clic en “Siguiente"	
Acepta las condiciones de licencia Haga clic en Siguiente"	

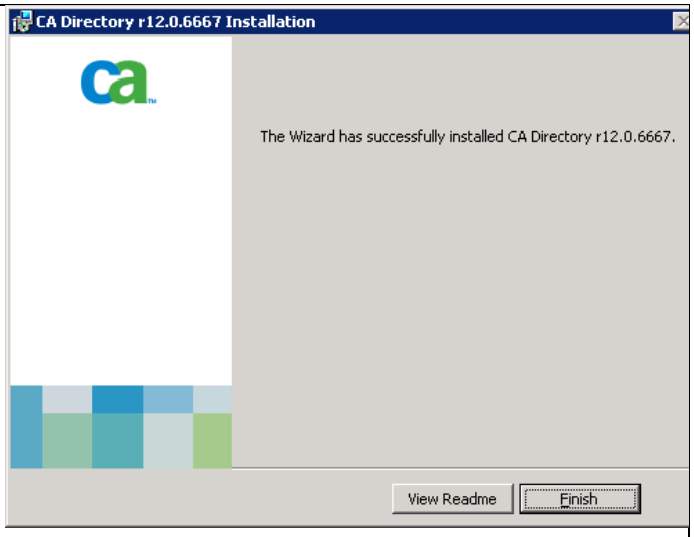
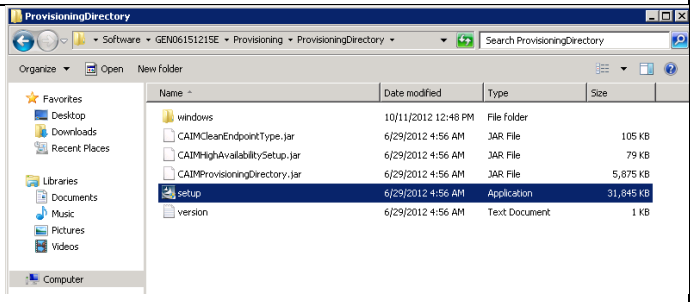
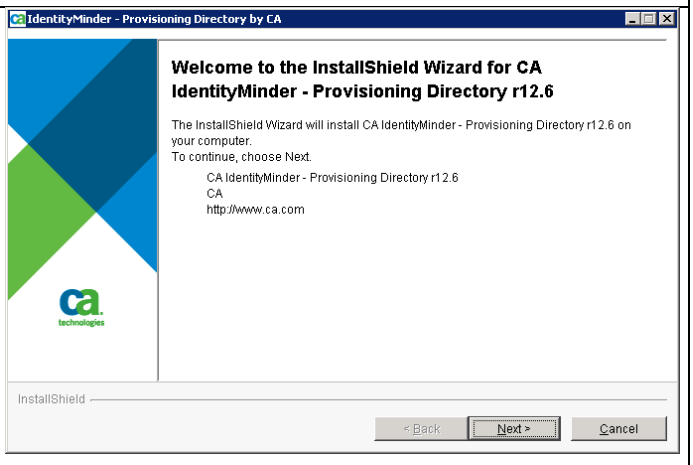
327

Elija instalación personalizada Haga clic en Siguiente"	
Cambie el destino para instalar en la unidad "D "	
Haga clic en Siguiente"	

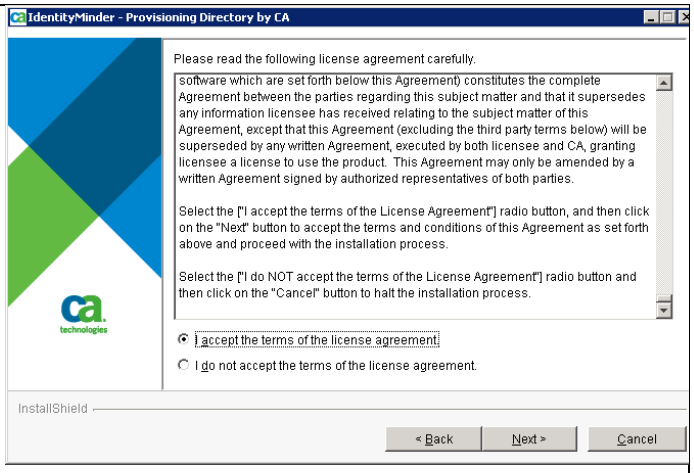
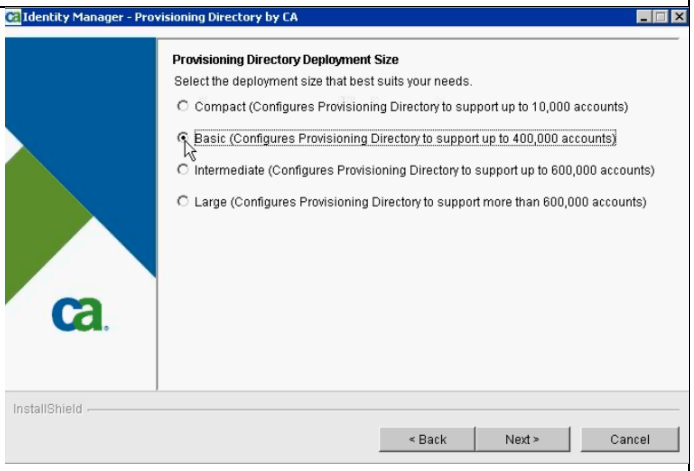
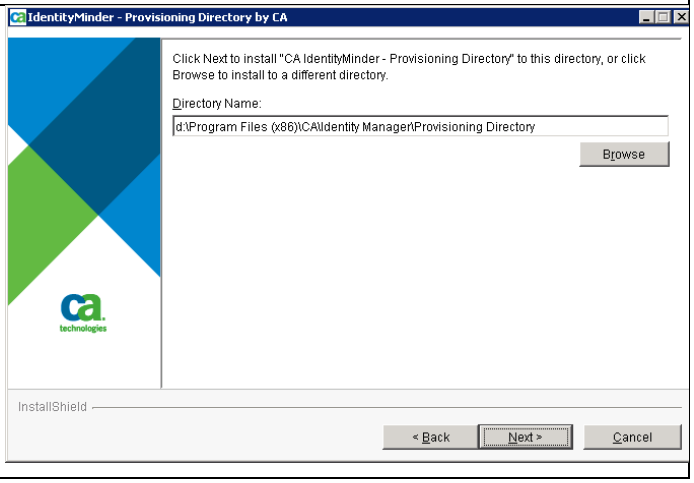
328

Desactive la casilla Dxmanager	
Revisión y ajustes Haga clic en Siguiente"	
Seleccione instalar	

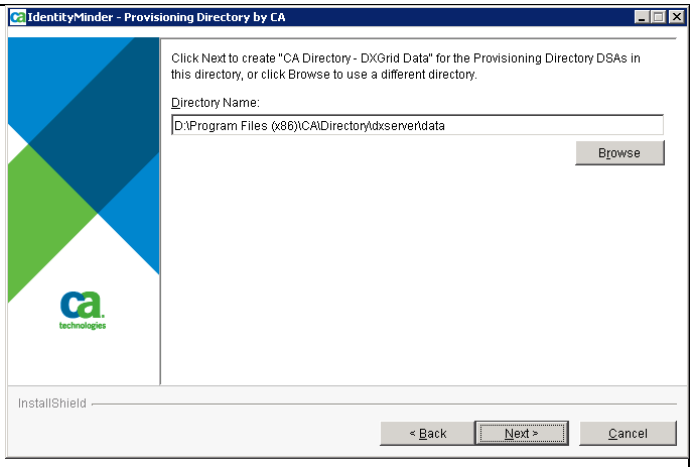
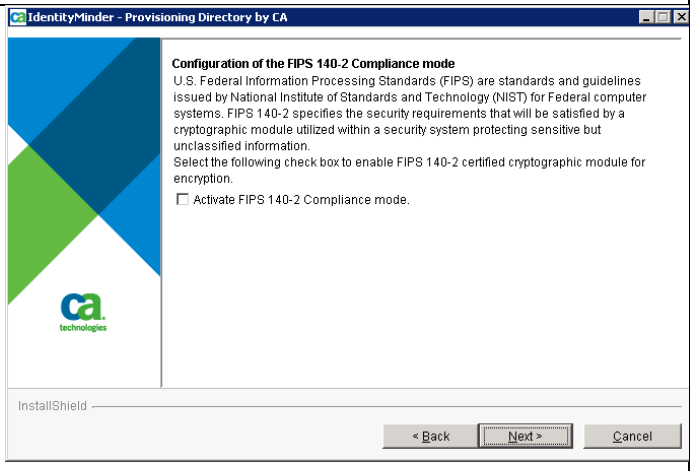
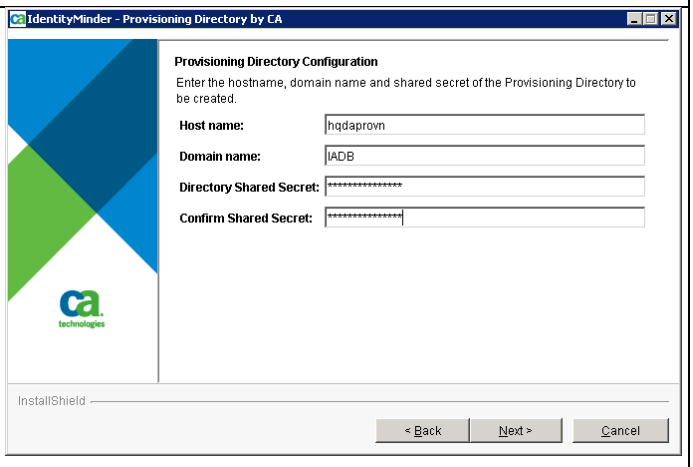
329

La instalación completaría y usted ver la pantalla a la derecha. Haga clic en " Finalizar"	
Inicie el instalador para el directorio de aprovisionamiento mediante la ejecución de ' setup.exe ' como administrador en "D: \ Software \ GEN06151215E \ \ Provisioning \ ProvisioningDirectory "	
Haga clic en Siguiente"	

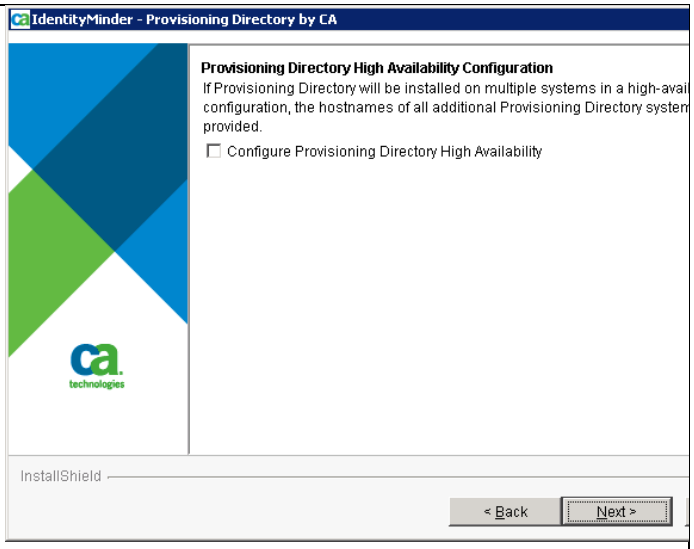
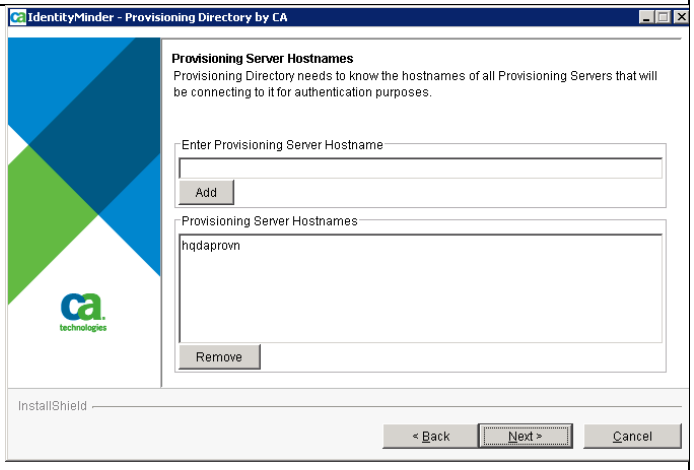
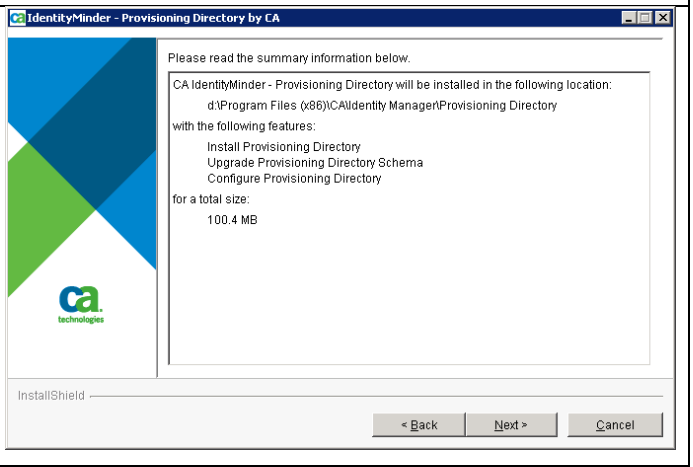
330

Seleccione "Acepto los términos del acuerdo de licencias " y Haga clic en Siguiente"	
Selecciona básico y Haga clic en Siguiente"	
Cambie el destino para instalar en la unidad "D "	

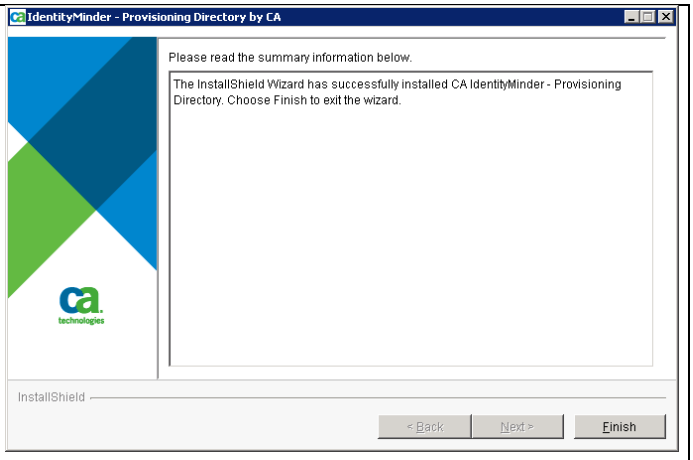
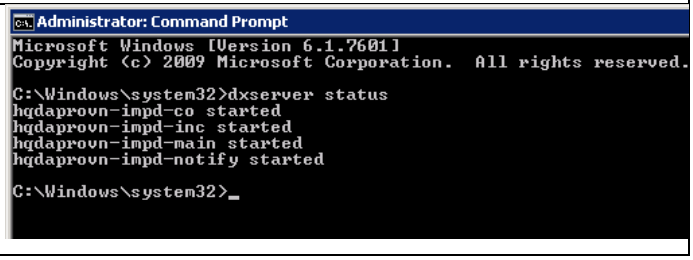
331

Cambie el destino para instalar en la unidad "D "	
Desmarque la casilla de verificación para desactivar el modo de cumplimiento de FIPS. Haga clic en Siguiente"	
Introduzca el nombre de host como se muestra en la imagen con información específica del servidor	

332

Desactive la opción " Configuración de aprovisionamiento Directorio de alta disponibilidad " Haga clic en " Siguiente"	
" Haga clic en " Siguiente"	
Revise los ajustes de instalación . " Haga clic en " Siguiente"	

333

La instalación sería proceder y completar con éxito . Haga clic en " Finalizar"	
En un símbolo del sistema ventana de ejecución " dxserver estado " para verificar que todos los ASD están ejecutando	

2.1.4 Instación de servidor abastecimiento

En la máquina del 'CA Provisioning Server ' , inicie la sesión como "Administrador" para completar la instalación .

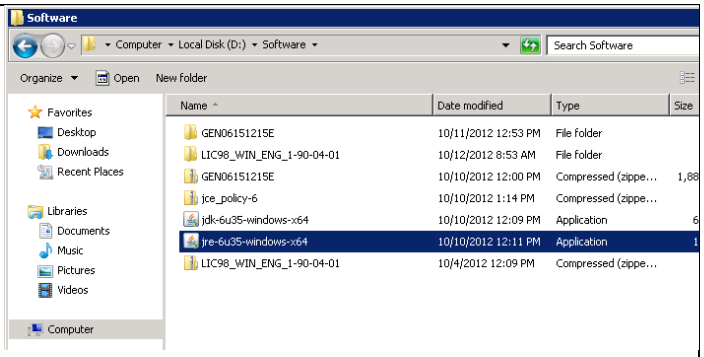
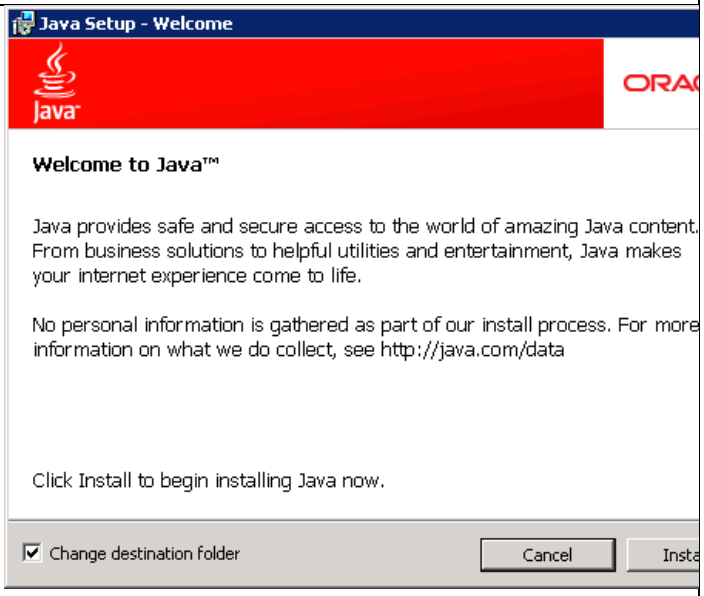
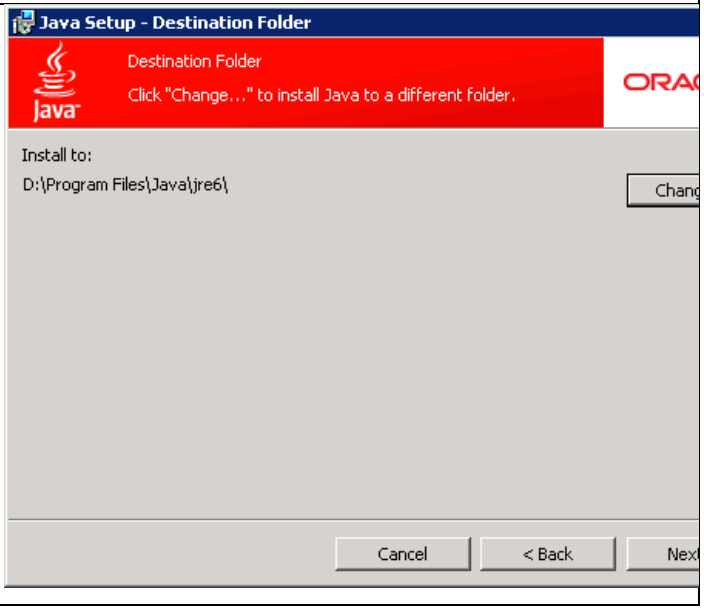
Requisitos de instalación

- El servidor de aprovisionamiento se debe instalar en la misma máquina en la que reside el directorio de aprovisionamiento.

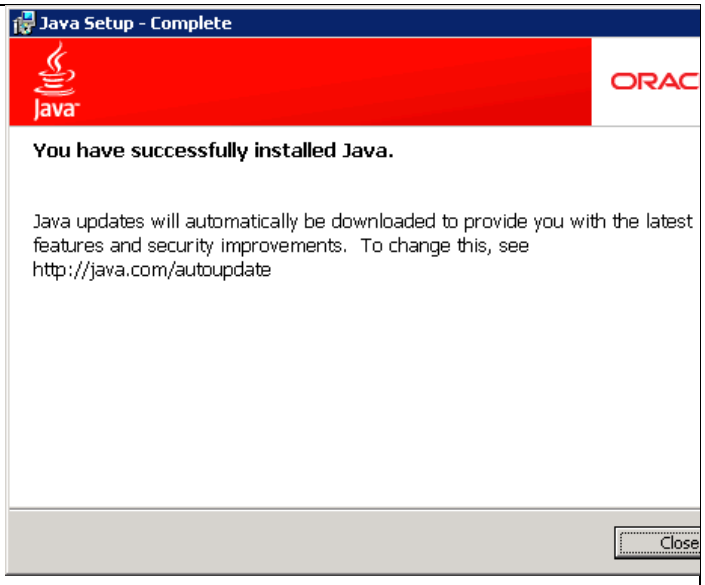
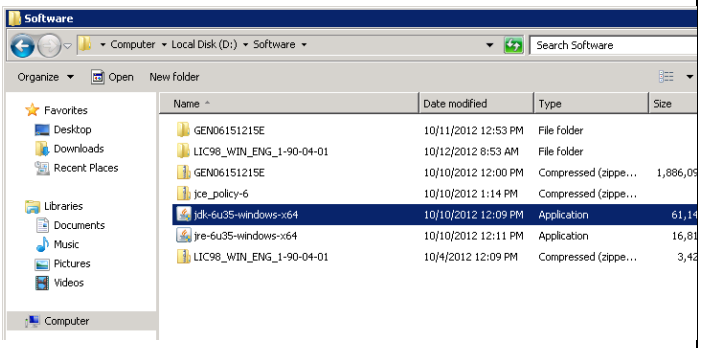
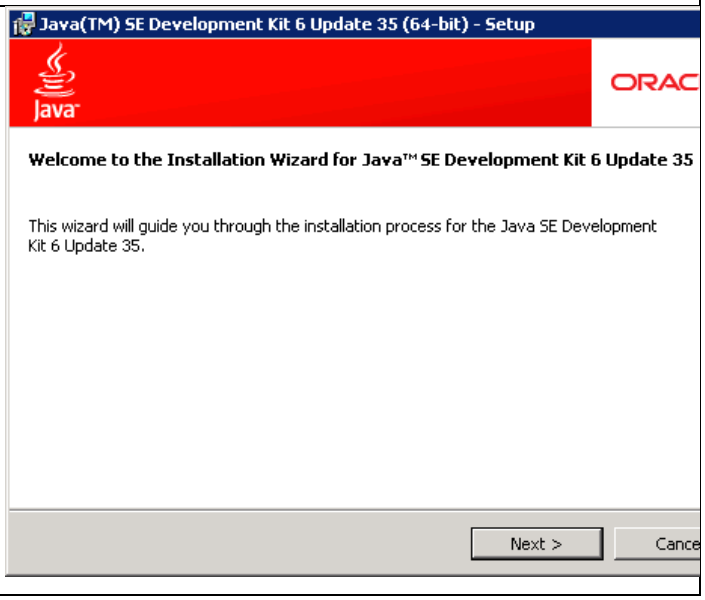
Pasos de instalación:

Instalar servidor de abastecimiento CA	
Instale el jre haciendo clic en el instalador obtenida de la página web de Oracle	

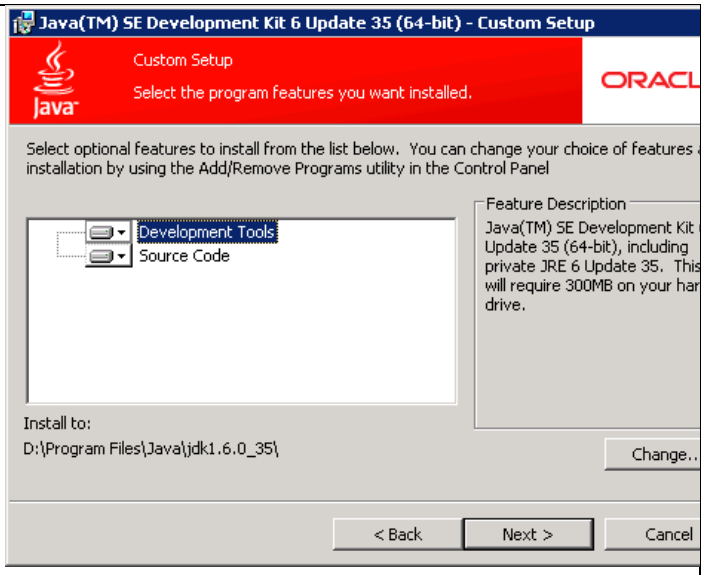
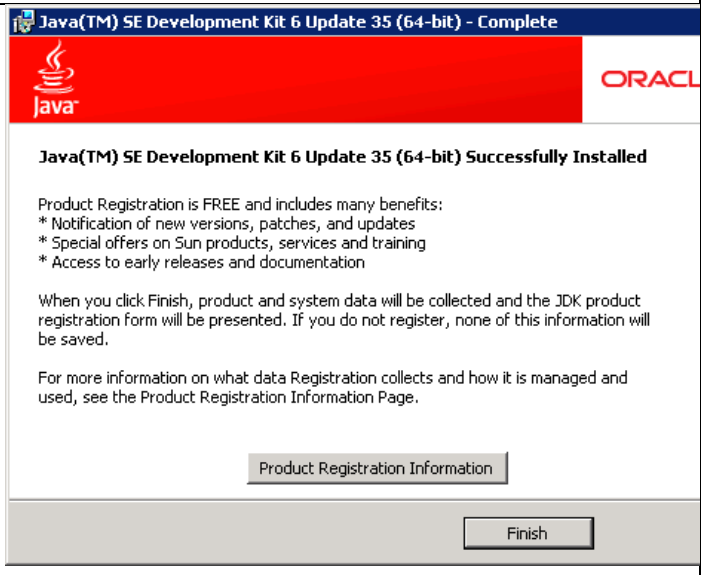
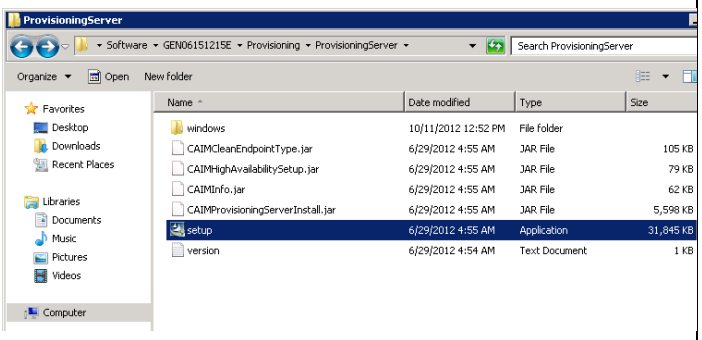
334

	
Marque la casilla para cambiar la carpeta de destino	
Asegúrese de que la carpeta de destino se establece en disco "D" y pulse Siguiente	

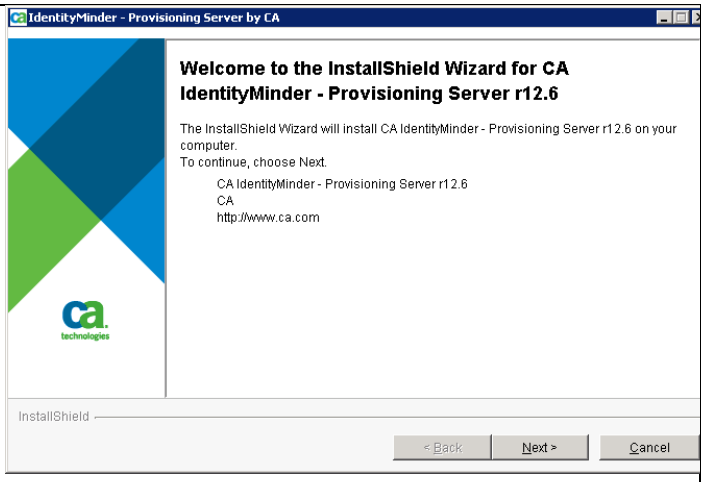
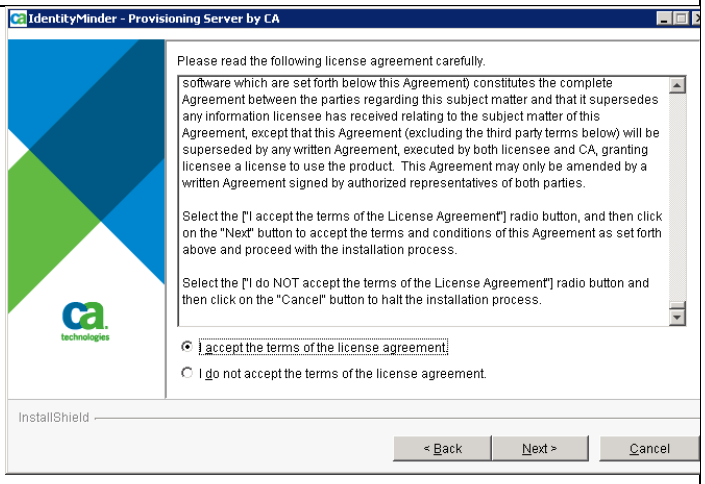
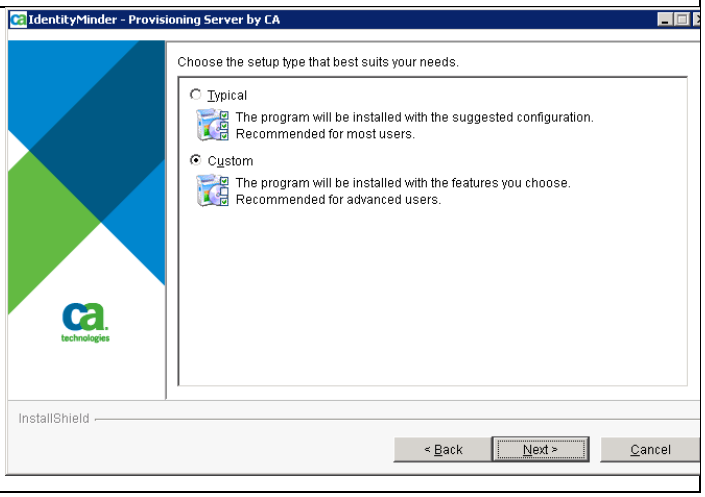
335

Después de la instalación se ha completado cerca del instalador	
Instale el JDK haciendo clic en el instalador obtenida de la página web de Oracle	
Haga clic en Siguiente	

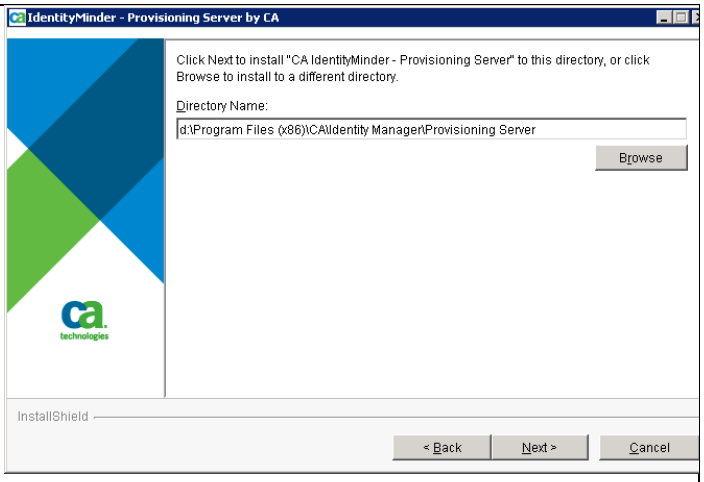
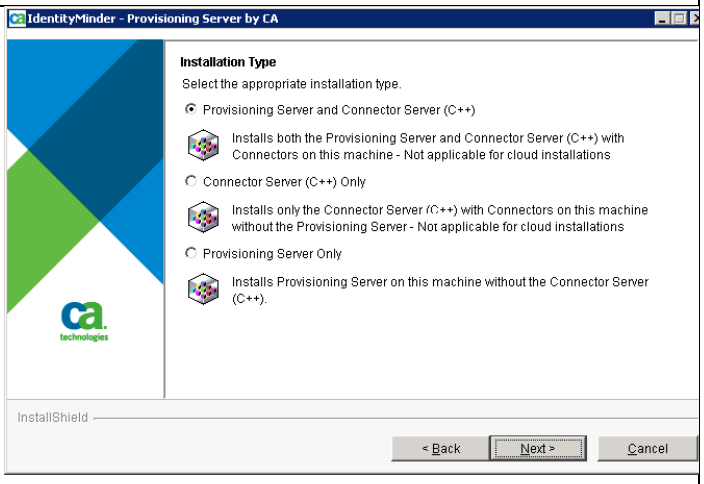
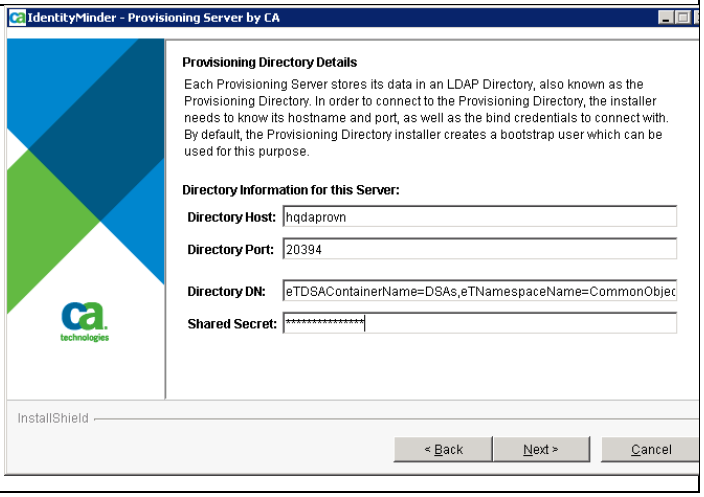
336

Asegúrese de que la carpeta de destino se establece en disco "D" y pulse Siguiente	
Después de la instalación se haya acabado completa Haga clic para cerrar el instalador	
Inicie el instalador para Provisioning Server ejecutando ' setup.exe ' como " Administrador" en D : \ Software \ GEN06151215E \ Provisioning \ ProvisioningServer	

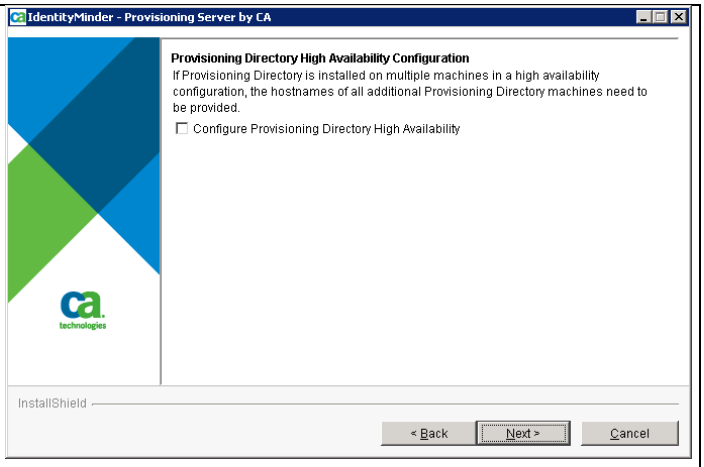
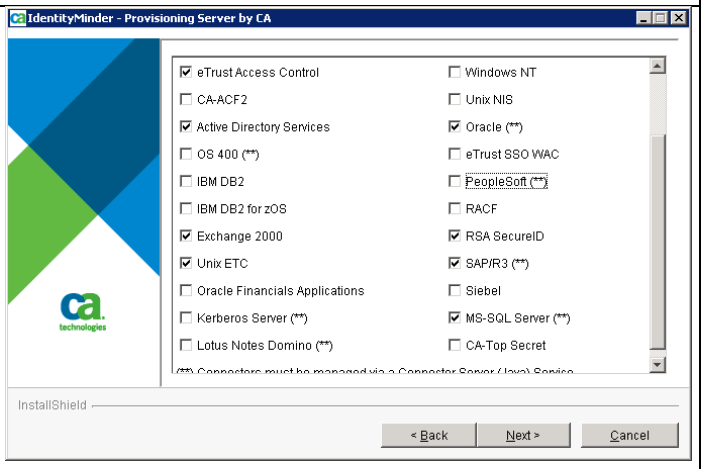
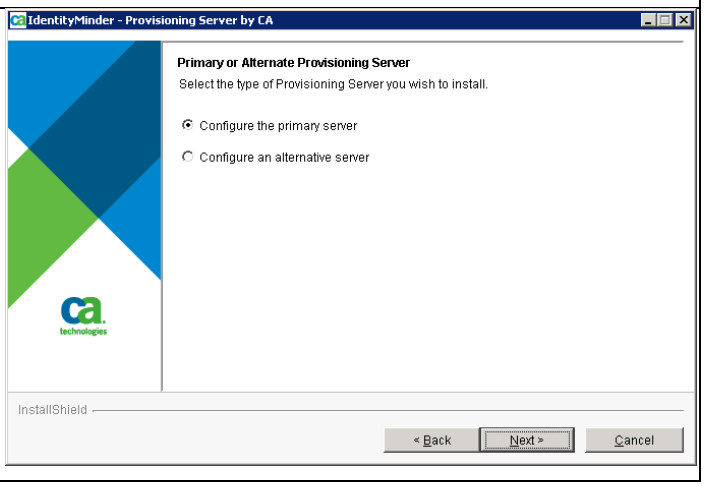
337

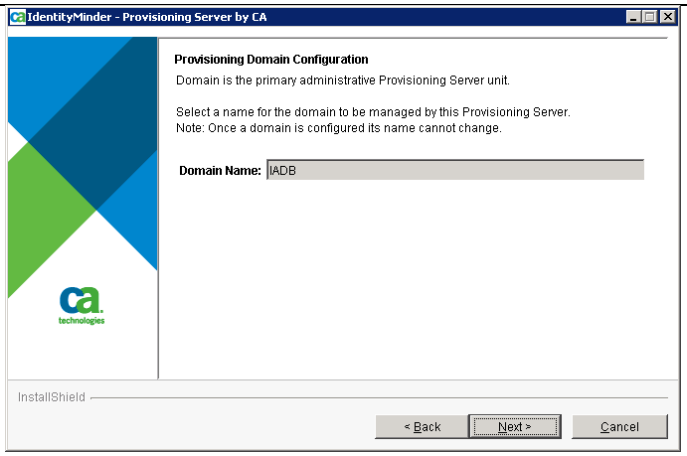
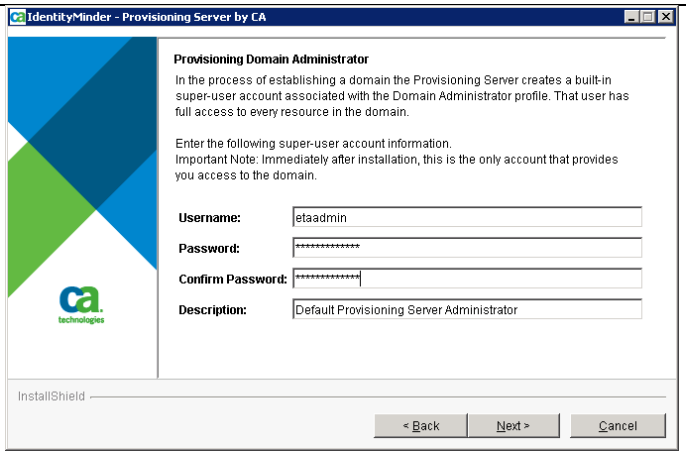
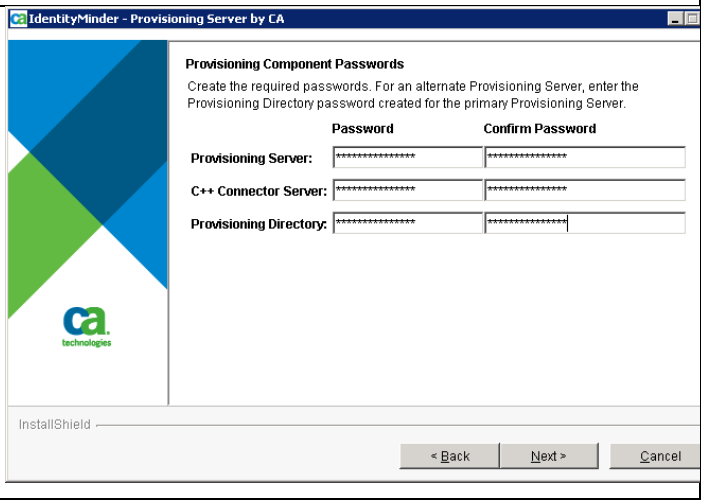
Haga clic en Siguiente"	
Seleccione " Acepto los términos del acuerdo de licencia " y haga clic en "Siguiente "	
Elija la instalación "Personalizada " . Haga clic en Siguiente"	

338

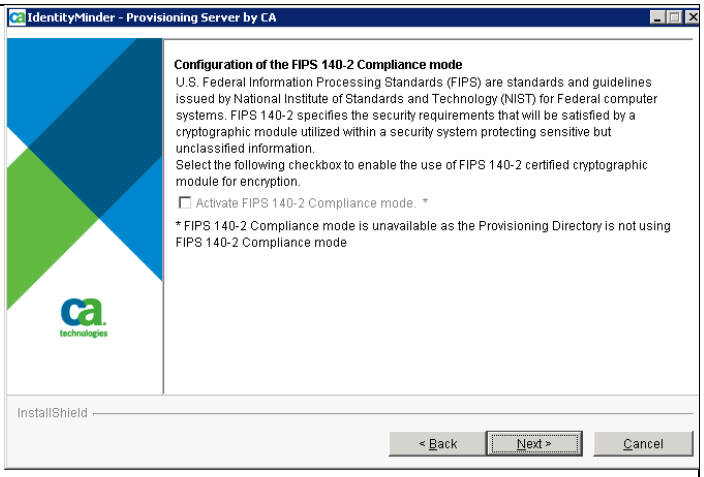
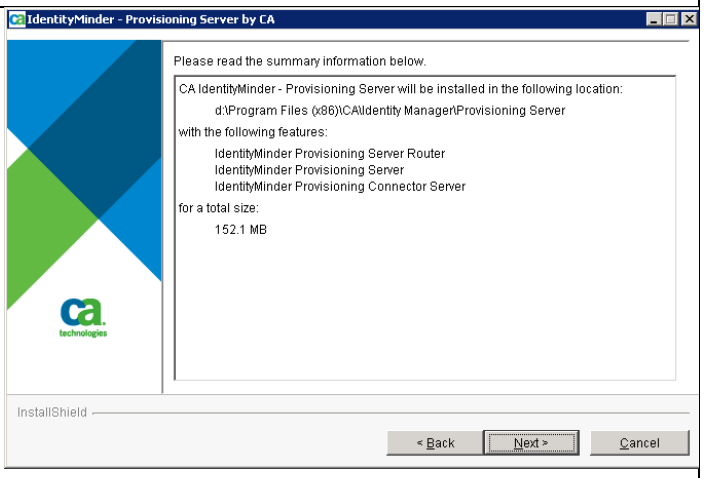
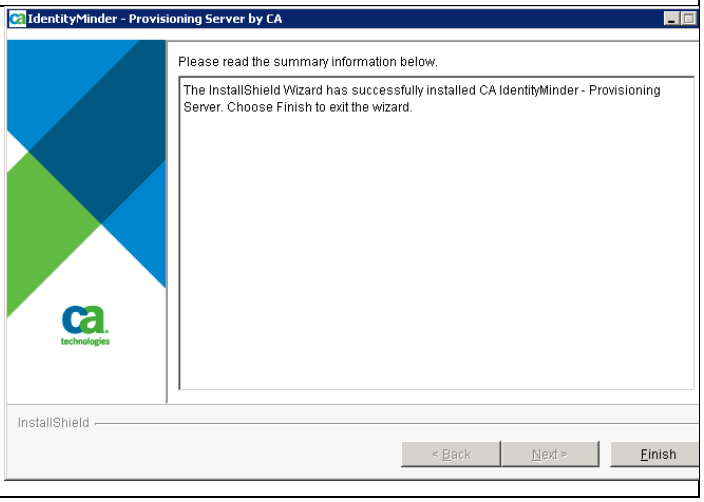
Cambie el directorio para instalar en la unidad "D "	
Elija el tipo de instalación como " servidor de aprovisionamiento y conector Server" . Haga clic en Siguiente"	
Proporcionar los detalles Directorio de aprovisionamiento como muestra en la imagen con la información del directorio de aprovisionamiento instalado en el paso anterior	

339

Desactive la casilla para alta disponibilidad	
Seleccione los conectores de aprovisionamiento que se utilizarán . Para BID la caja en la imagen muestra todos los componentes seleccionados durante la instalación .	
En la siguiente pantalla, seleccione " Configuración del servidor principal " . Haga clic en Siguiente"	

Elija el dominio para el servidor de aprovisionamiento . Dominio: " BID " Haga clic en Siguiente"	
Introduzca los detalles de aprovisionamiento de dominio . Haga clic en Siguiente"	
Introduzca las contraseñas para todos los componentes de aprovisionamiento .	

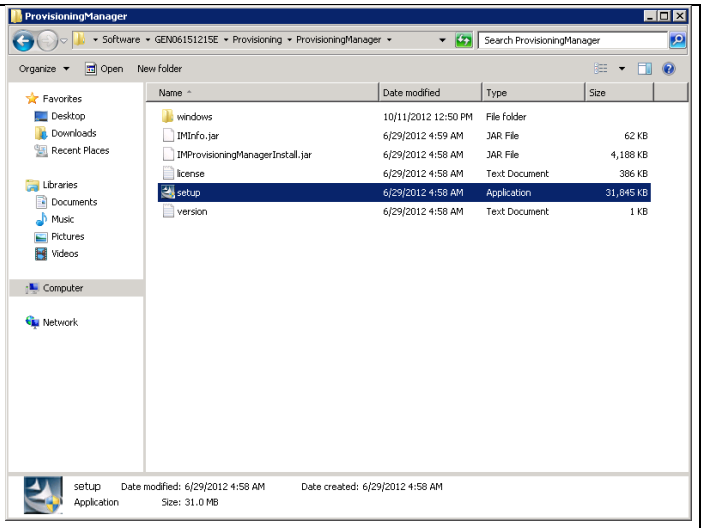
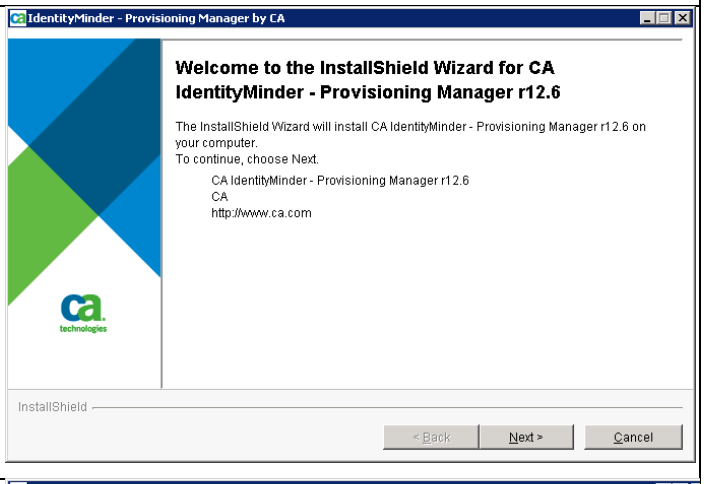
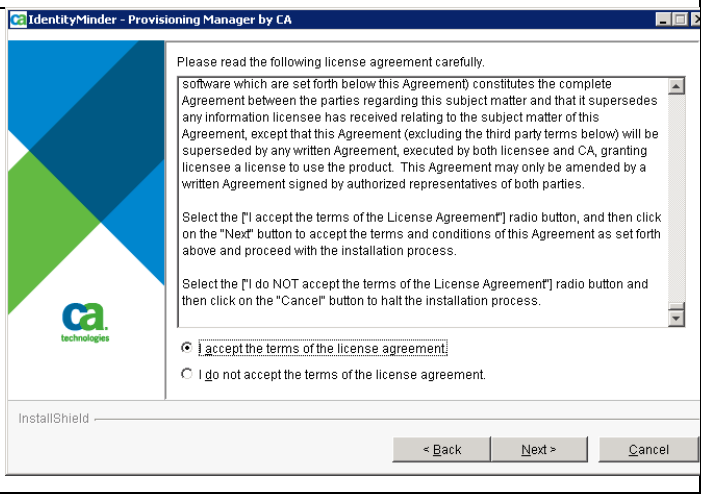
341

Hacer "modo de cumplimiento de FIPS " Seguro no esté marcada . Haga clic en Siguiente"	
Revise los ajustes de instalación . Haga clic en Siguiente" La instalación sería proceder y completar con éxito .	
El procedimiento de instalación está completa. Haga clic en " Finalizar"	

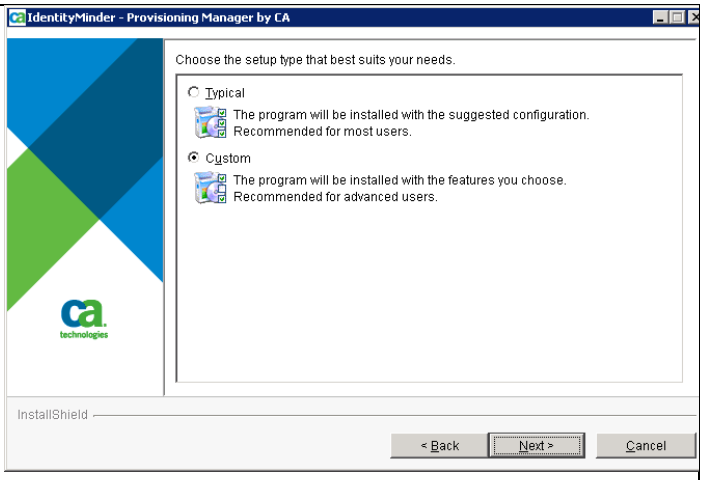
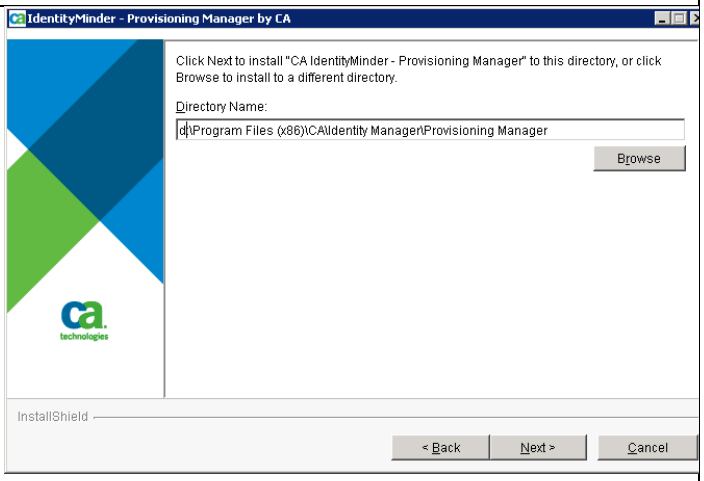
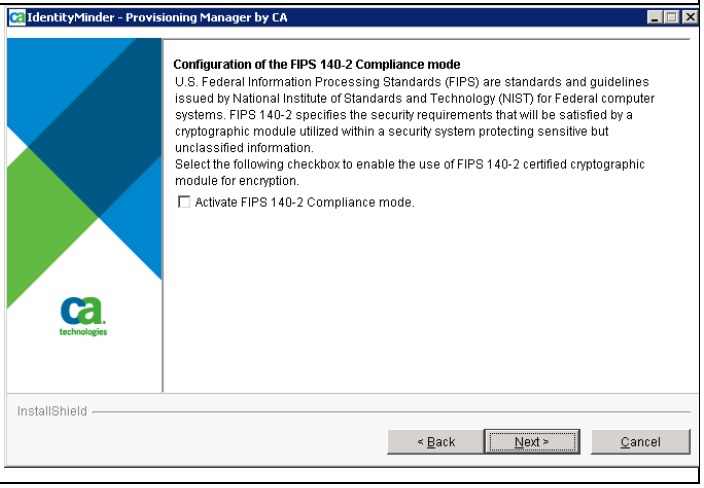
19.1.5 Instalación Provisioning Manager

Instalación de CA Provisioning Manager

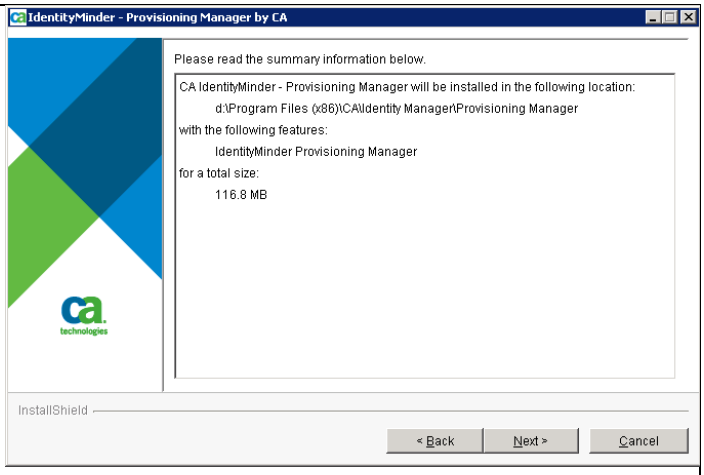
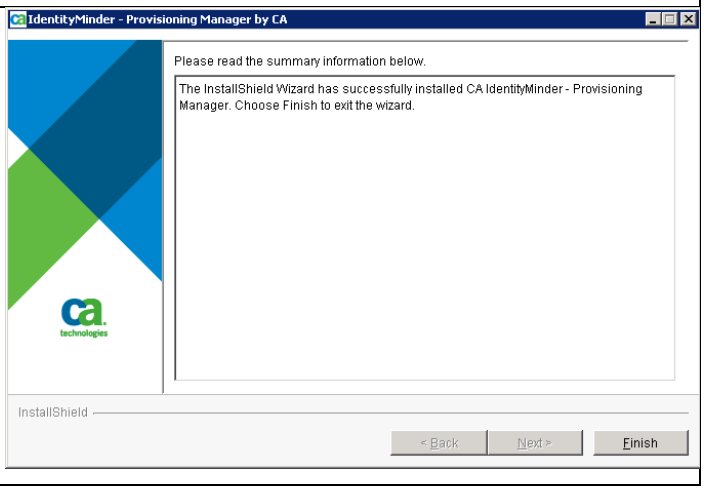
342

Inicie el instalador para Provisioning Server ejecutando ' setup.exe ' como " Administrador" en D: \ Software \ GEN06151215E \ Provisioning \ ProvisioningManager	
Haga clic en Siguiente"	
Acepte el acuerdo de licencia. Haga clic en Siguiente"	

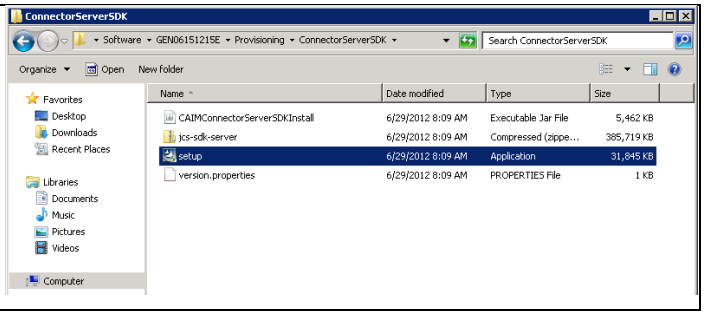
343

Elija instalación personalizada . Haga clic en Siguiente"	
Cambie el directorio de instalación de la unidad "D "	
No Compruebe FIPS 140-2 modo Cumplimiento Activar. Haga clic en Siguiente"	

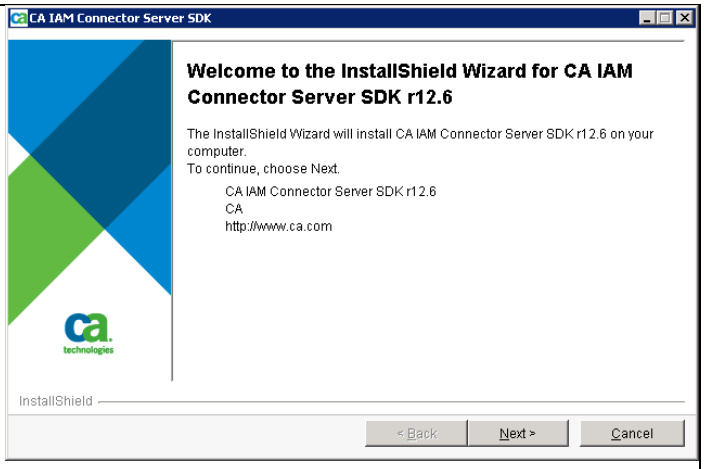
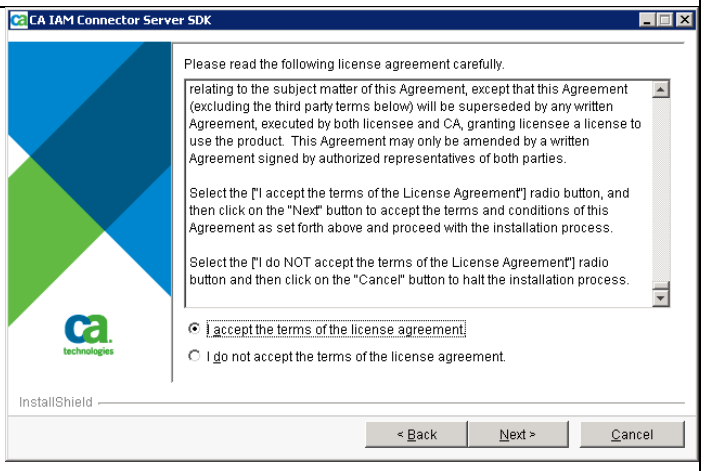
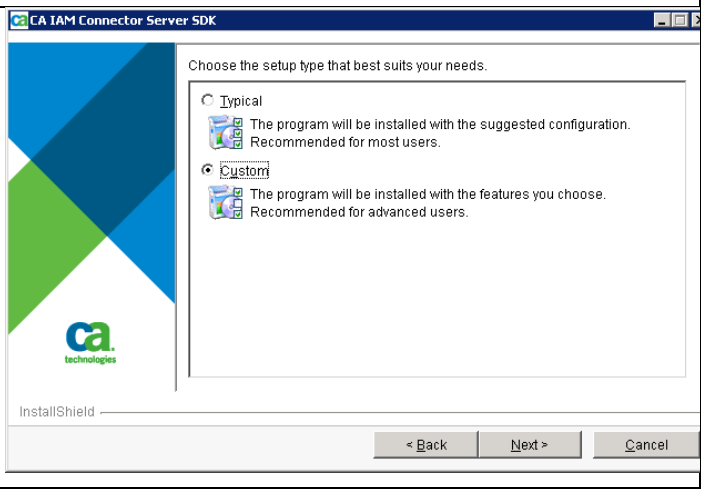
344

Haga clic en Siguiente para aceptar los detalles de la instalación . Haga clic en Siguiente"	
La instalación sería proceder y completar con éxito . Haga clic en " Finalizar" .	

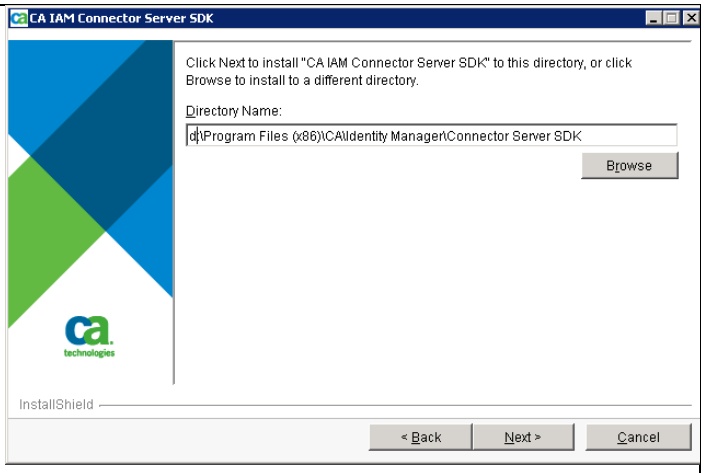
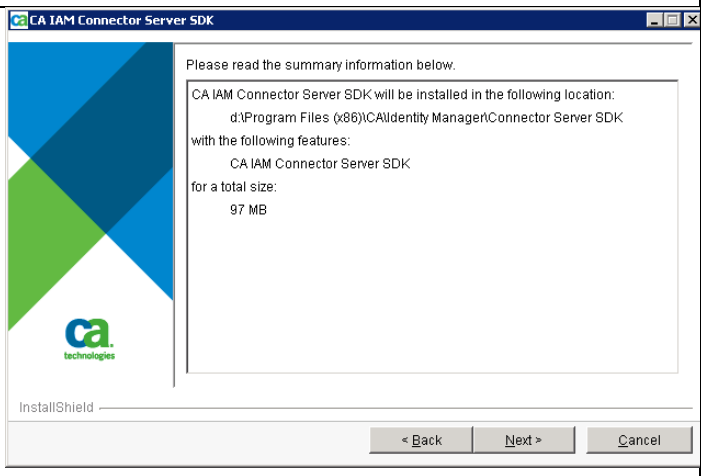
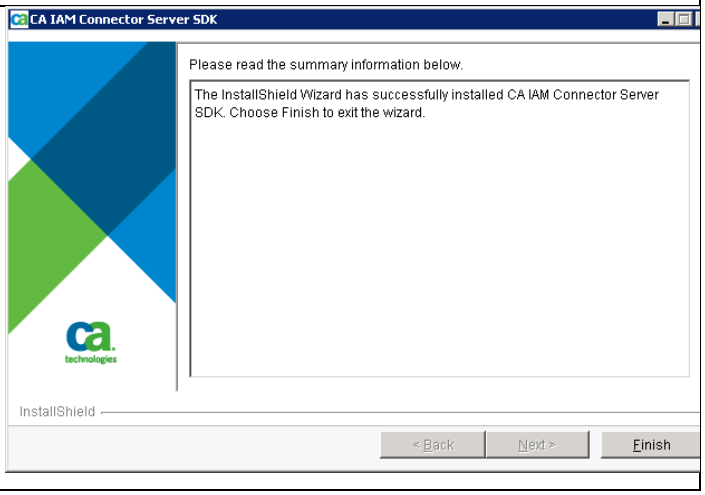
2.1.5 Instalacion de conector servidor SDK

Inicie el instalador para Provisioning Server ejecutando ' setup.exe ' como " Administrador" en D: \ Software \ GEN06151215E \ Provisioning \ConnectorServerSDK	

345

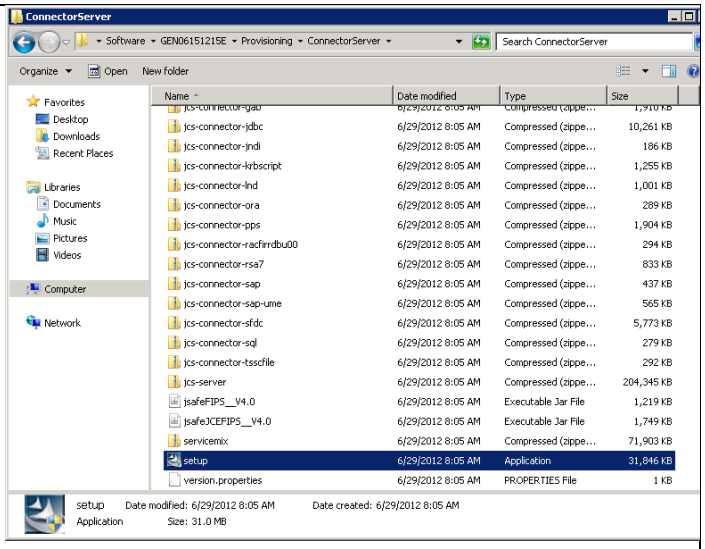
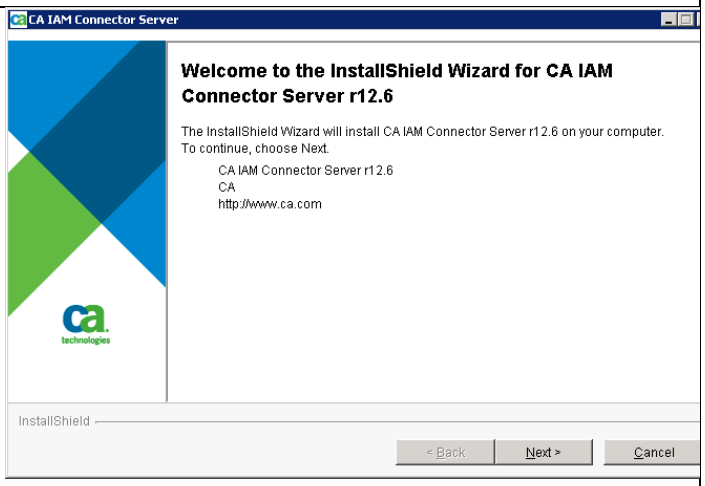
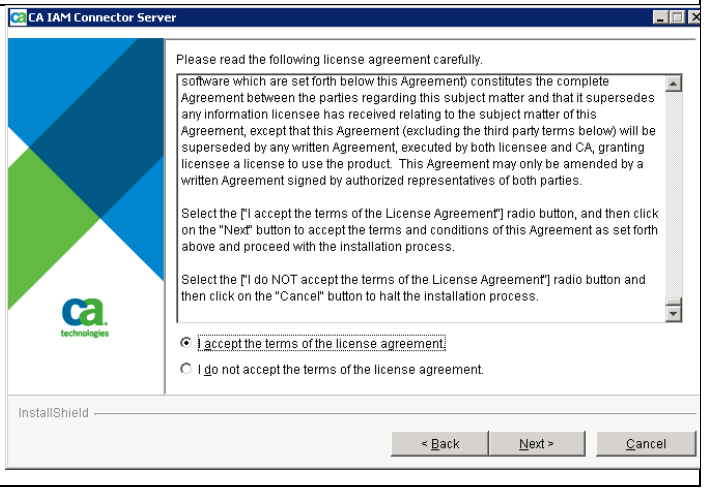
Haga clic en Siguiente"	
Acepte el acuerdo de licencia. Haga clic en Siguiente"	
En el tipo de instalación , seleccione : "Personalizado" Haga clic en Siguiente"	

346

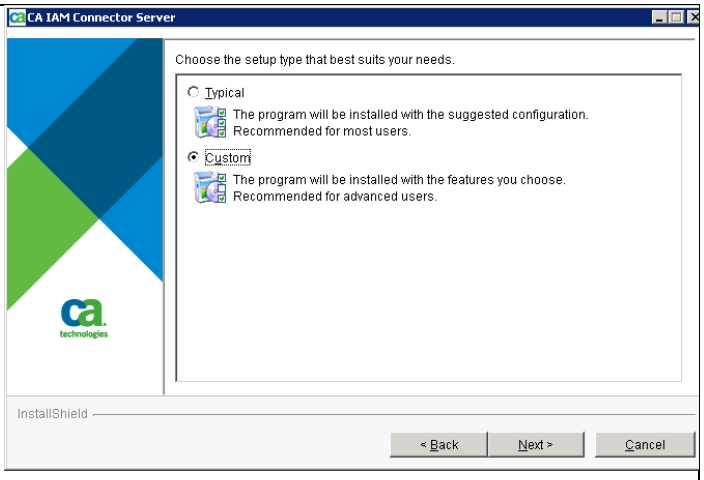
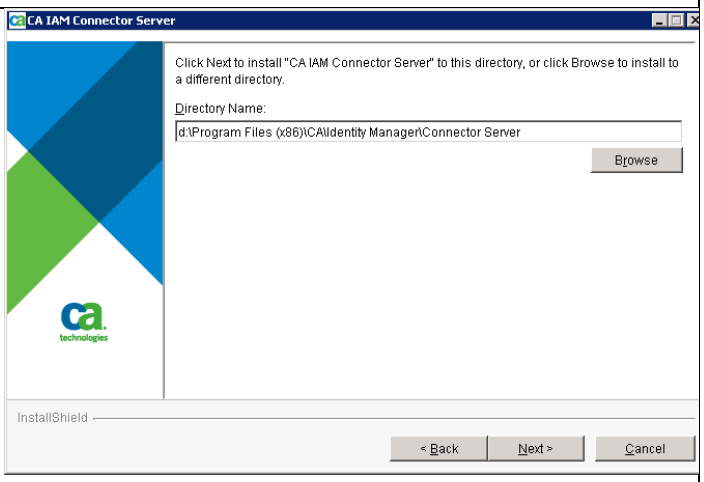
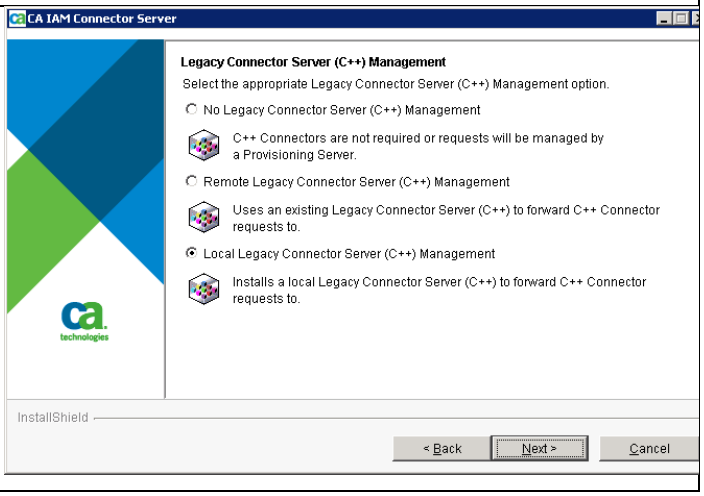
Cambiar la ruta de instalación en la unidad "D "	
Haga clic en Siguiente para aceptar los detalles de la instalación . Haga clic en Siguiente"	
La instalación sería proceder y completar con éxito . Haga clic en Finalizar	

2.1.6 Instalar Connector Server

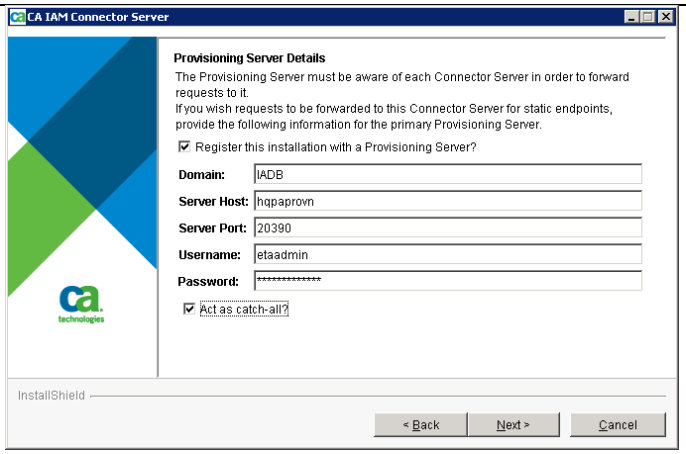
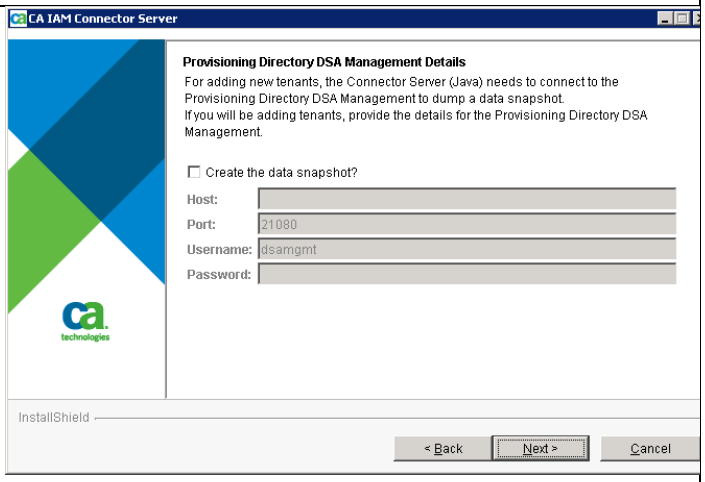
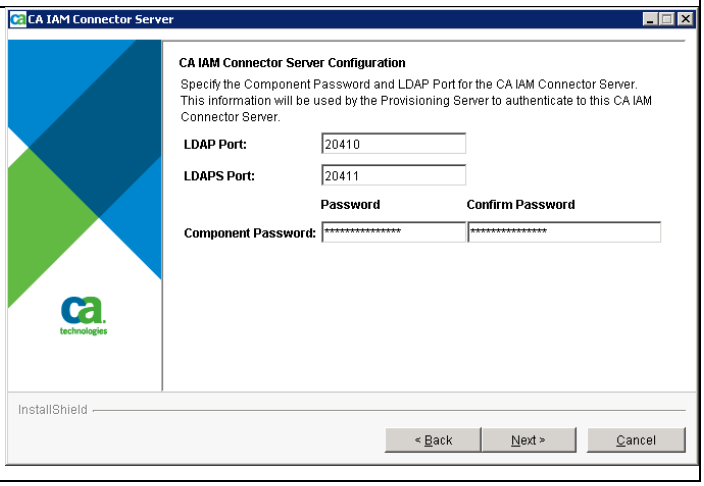
347

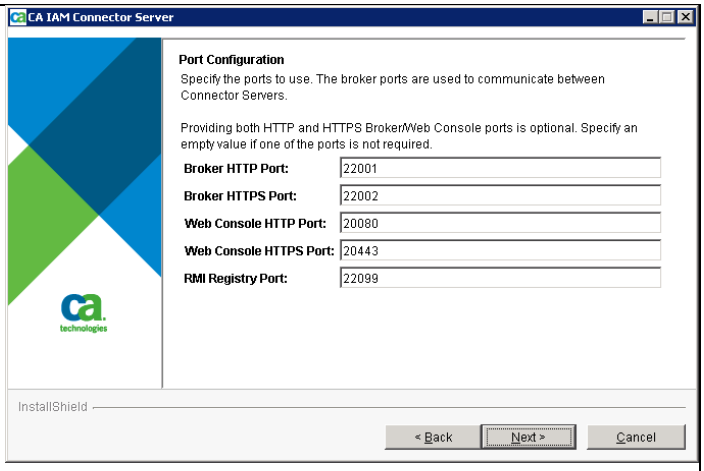
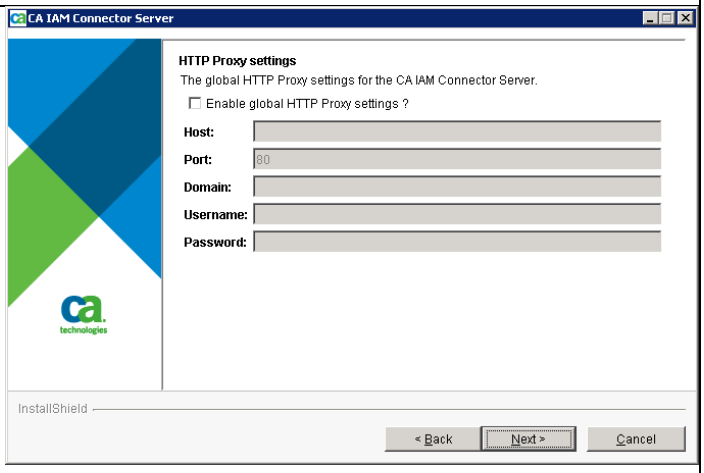
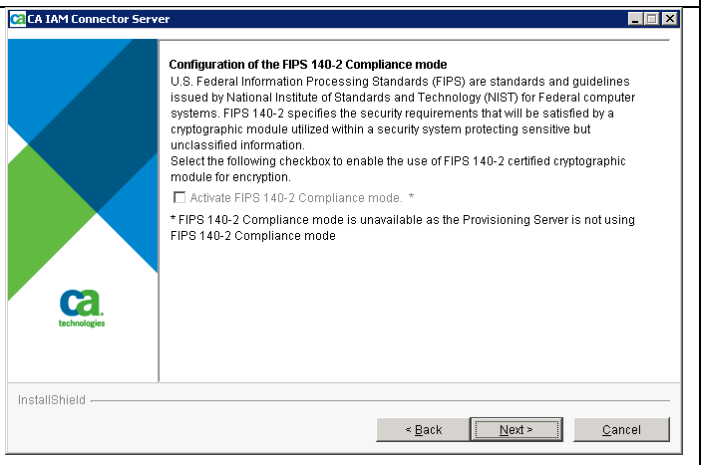
Inicie el instalador para Provisioning Server ejecutando ' setup.exe ' como " Administrador" en D: \ Software \ GEN06151215E \ Provisioning \ ConnectorServer	
Haga clic en Siguiente"	
Acepte el acuerdo de licencia. Haga clic en Siguiente"	

348

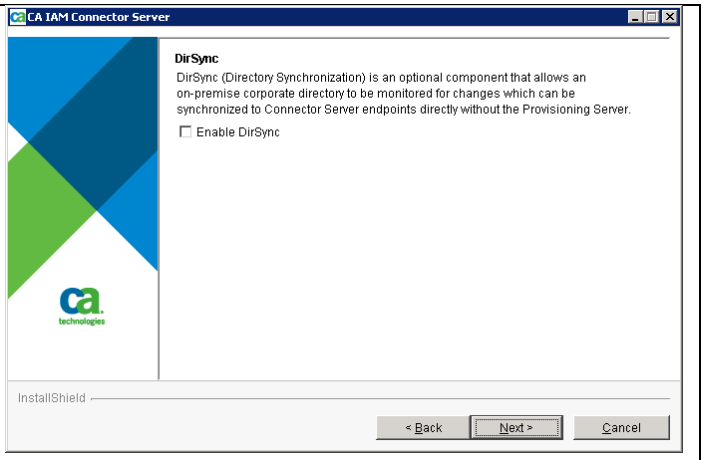
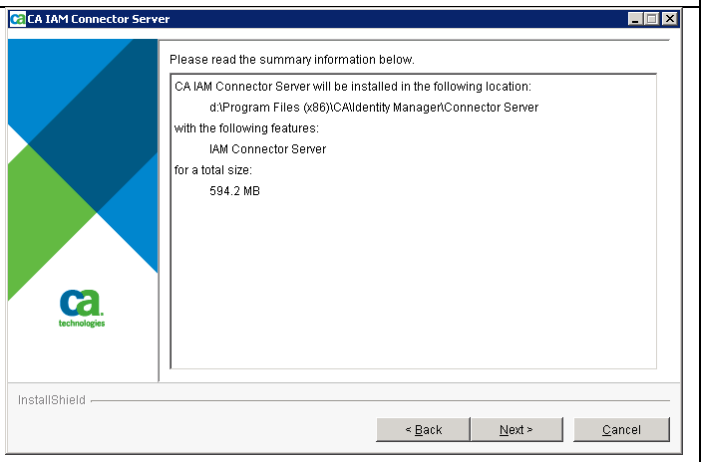
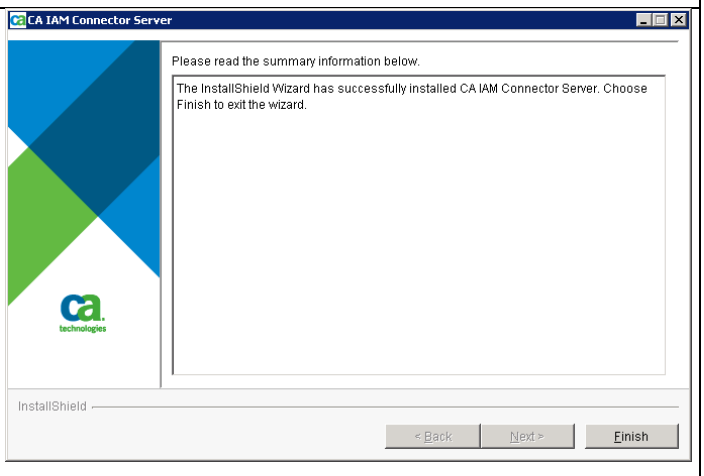
En el tipo de instalación , seleccione : "Personalizado" Haga clic en Siguiente"	
Cambiar la ruta de instalación en la unidad "D "	
Seleccione "Servidor Legado Conector local"	

349

Introduzca la información sobre el servidor de aprovisionamiento y seleccione "Actúa como cajón de sastre "	
Desactive la casilla para crear instantánea de datos	
Especifique la contraseña de componente	

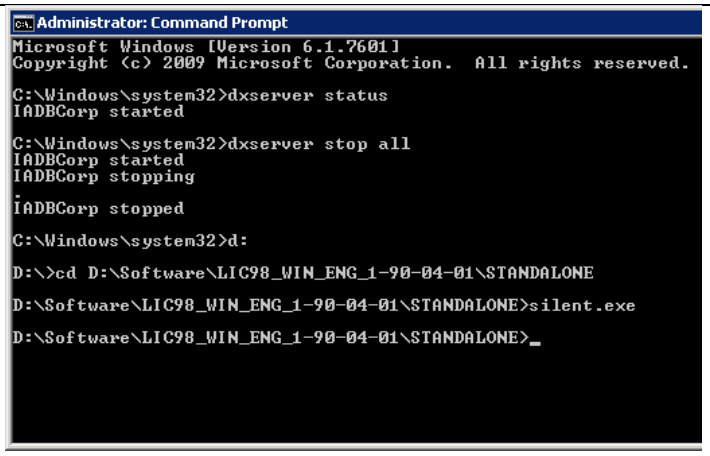
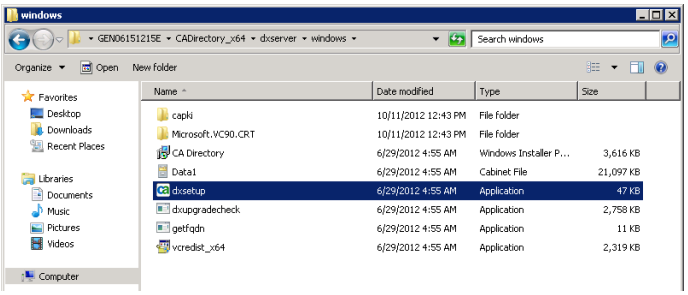
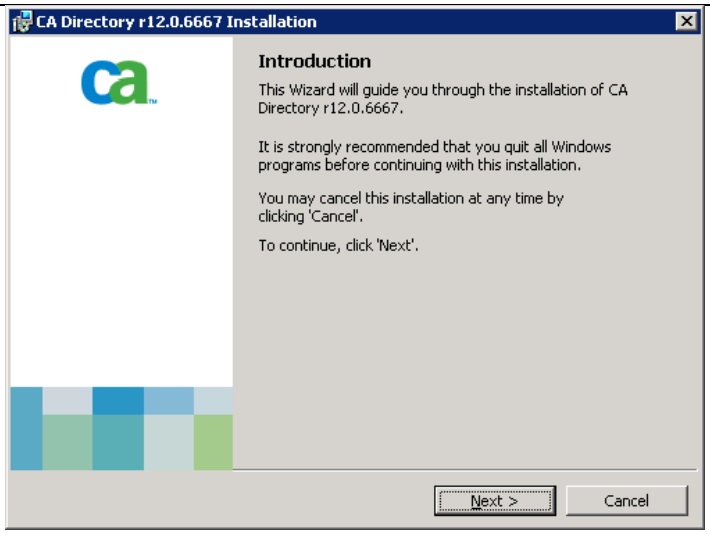
Verifique todos los puertos y haga clic en siguiente	
Desactive la opción " Habilitar la configuración de proxy HTTP global"	
Desactive la casilla para activar FIPS	

351

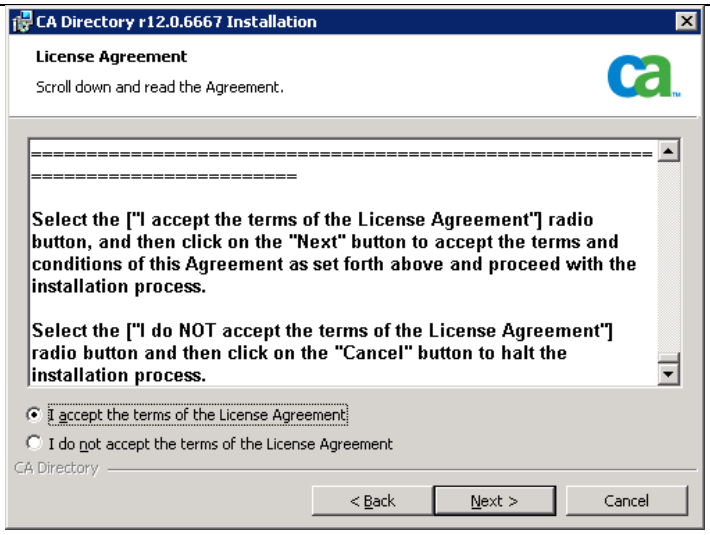
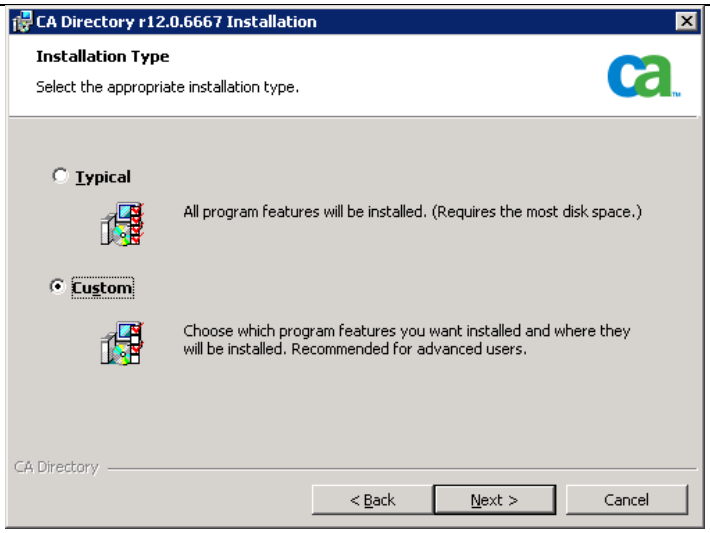
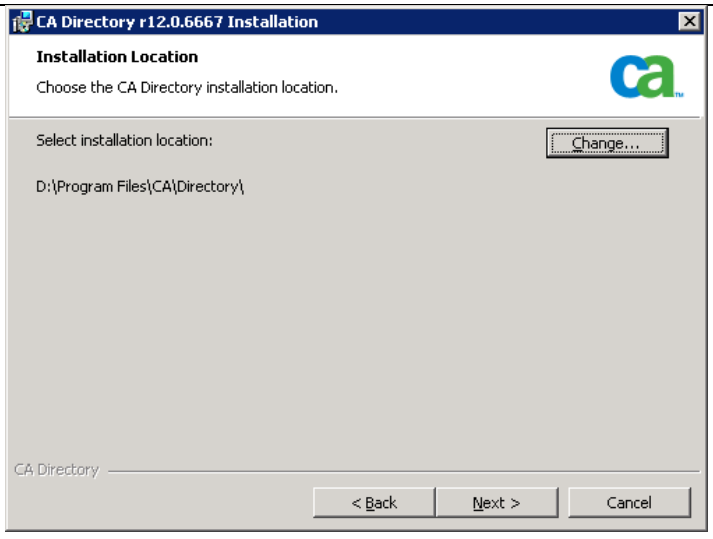
Desactive la casilla "Activar sincronización de directorios "	
Revise la instalación y haga clic en Siguiente	
Haga clic en Finalizar para salir del asistente	

352

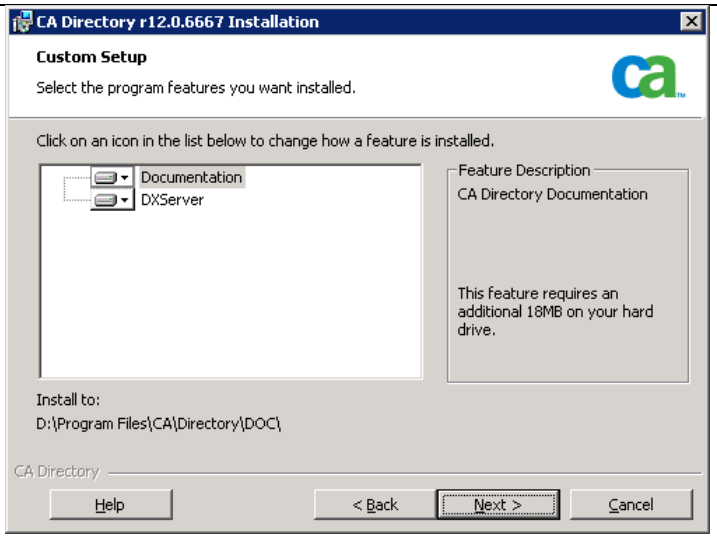
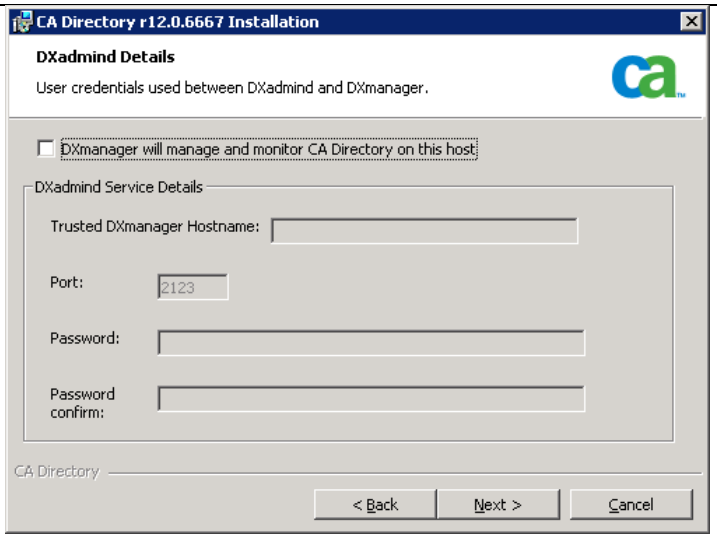
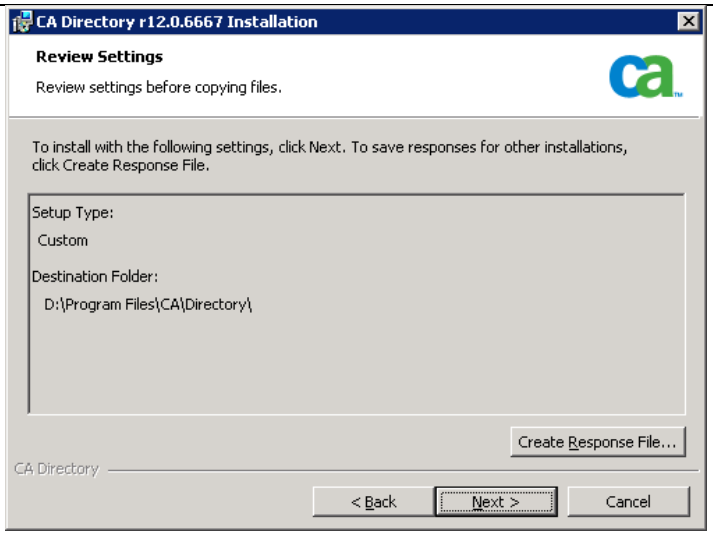
2.1.7 Instalar irectorio de CA Identity Minder Corporate

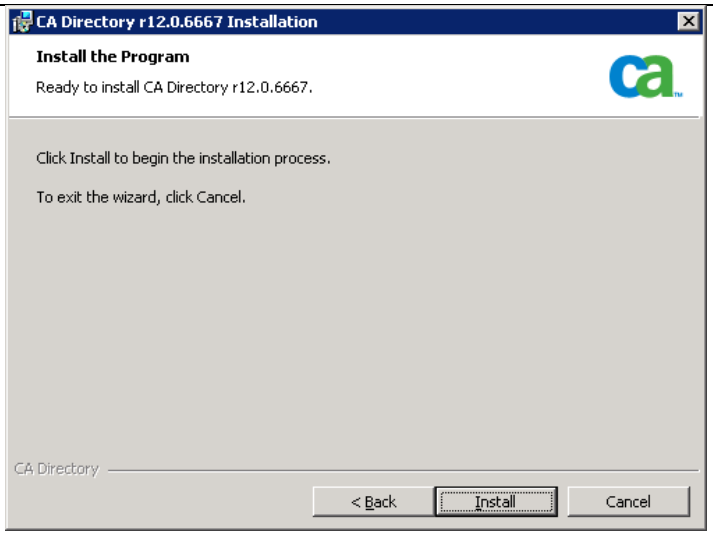
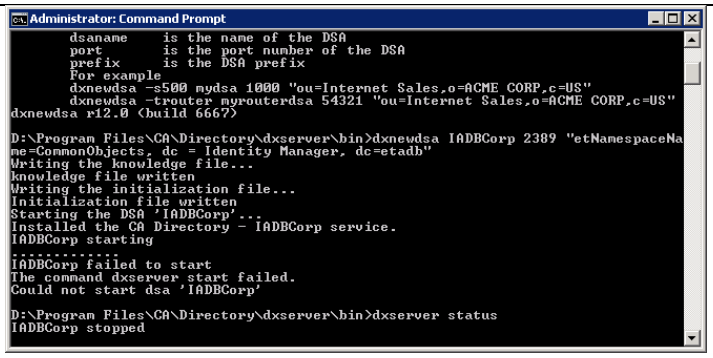
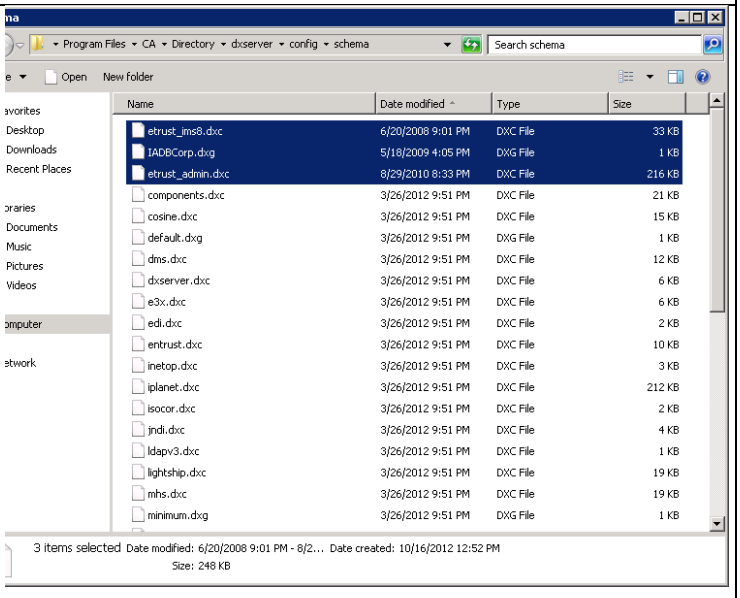
Instalar Directorio de CA Identity Manager Corporate	
En el servidor de aprovisionamiento, desde un símbolo del sistema ventana de exploración a D: \ Sotware \ LIC98_WIN_ENG_1-90-04-01 \ INDEPENDIENTE (O el equivalente en donde se instalan los archivos de licencia directorio) ejecutar silent.exe D. D especifica la unidad en la que desea que se instale a	
Busque la configuración de Directorio en "D: \ Software \ GEN06151215E \ CADirectory_x64 \ dxserver \ windows " Ejecute el archivo ' dxsetup.exe ' como " Administrador" .	
Haga clic en Siguiente"	

353

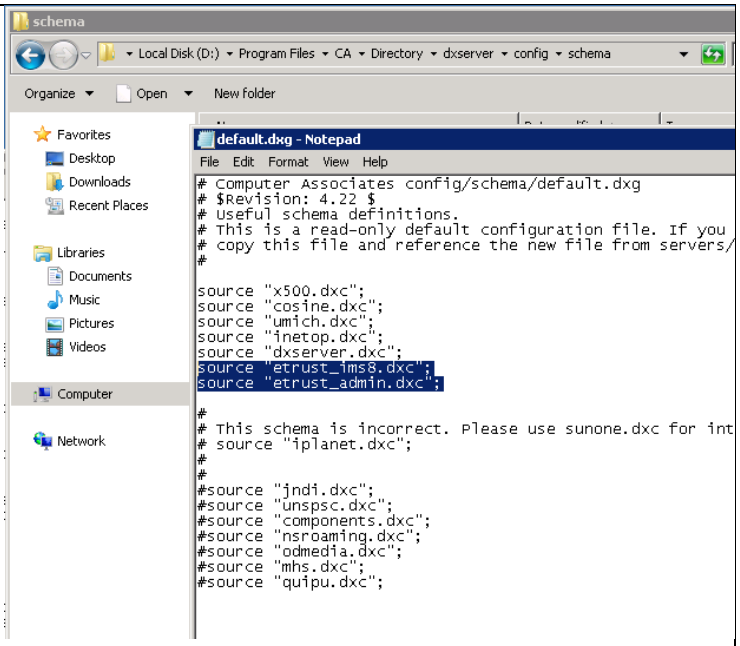
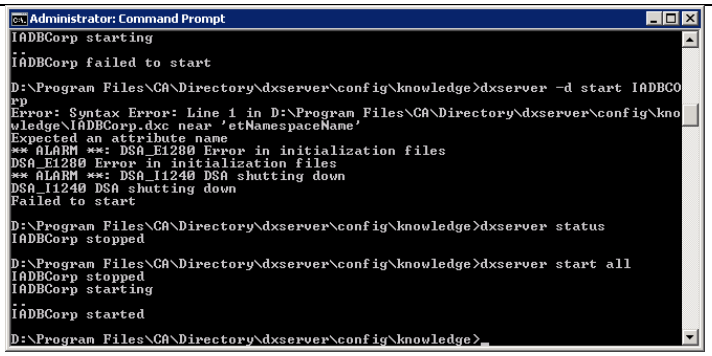
Acepta el Acuerdo de licencia de producto Haga clic en Siguiente"	
Elija la instalación " personalizada " . Haga clic en Siguiente"	
Cambie el destino para instalar debajo de la unidad "D "	

354

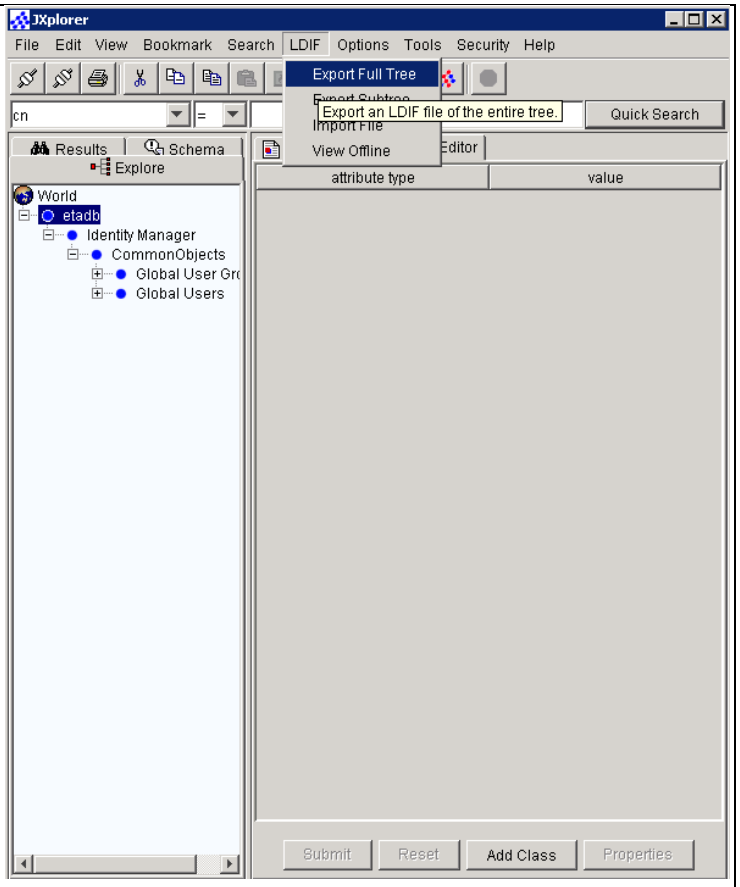
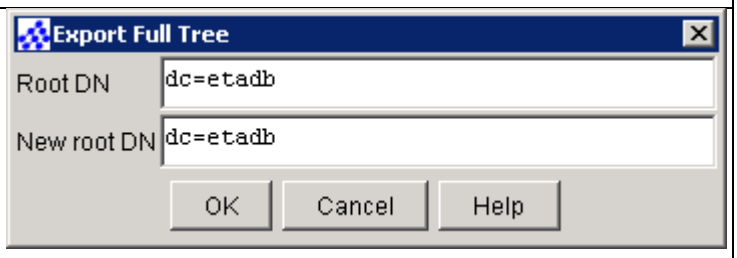
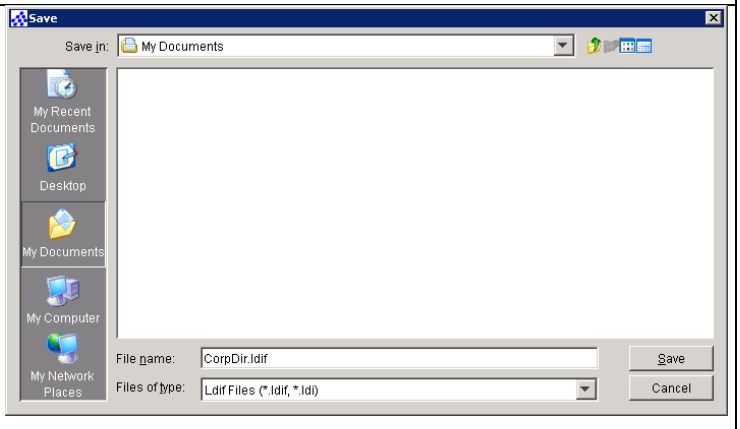
Haga clic en Siguiente"	
Desactive la casilla Dxmanager	
Revisión y ajustes Haga clic en Siguiente"	

Haga clic en " Instalar"	
Después de finalizada la instalación vaya a: D: \ Archivos de programa \ CA \ Directorio \ dxserver \ bin Escriba el siguiente comando para crear un DSA dxnewdsa IADBCorp 2389 " etNamespaceName = CommonObjects , dc = Identity Manager , dc = etadb	
Copia lo largo de los siguientes archivos en la pantalla del ambiente de edad para llevar sobre el esquema	

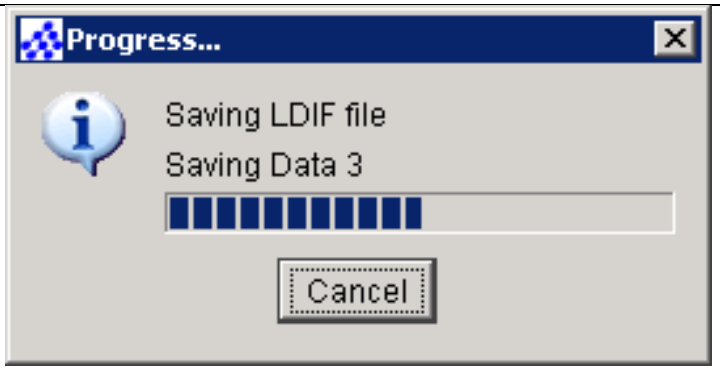
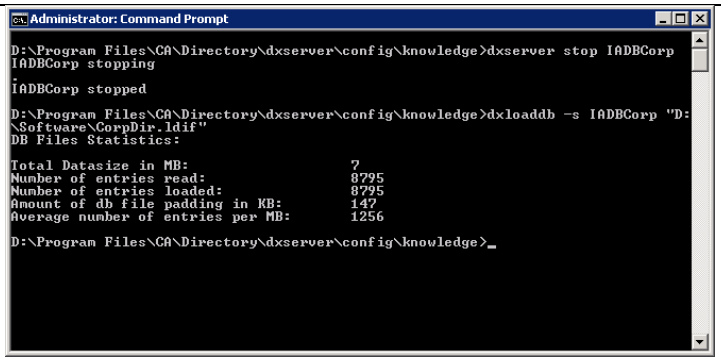
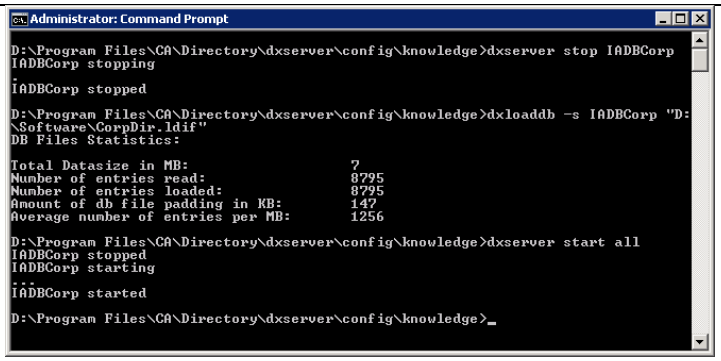
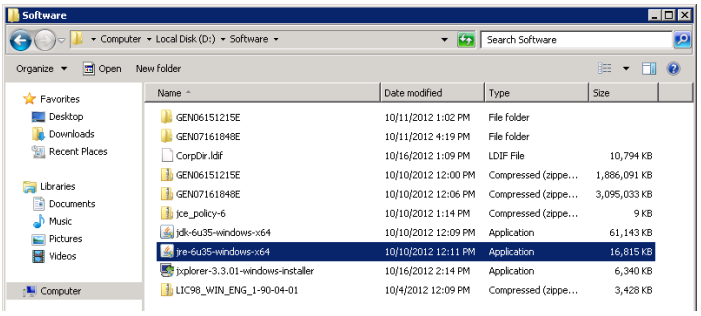
356

Vaya a D: \ Archivos de programa \ CA \ Directorio \ dxserver \ config \ esquema Abra default.dxg con bloc de notas y agregue las líneas resaltadas en la pantalla	
En un símbolo del sistema ventana de ejecución : Dxserver empezar	

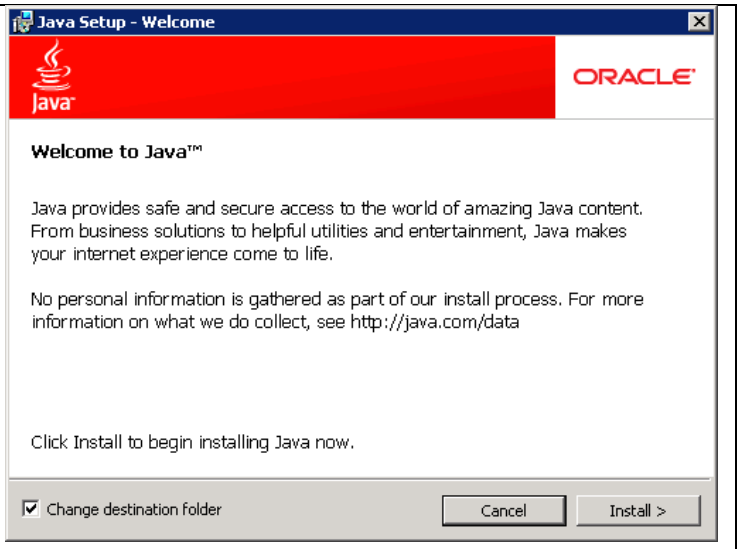
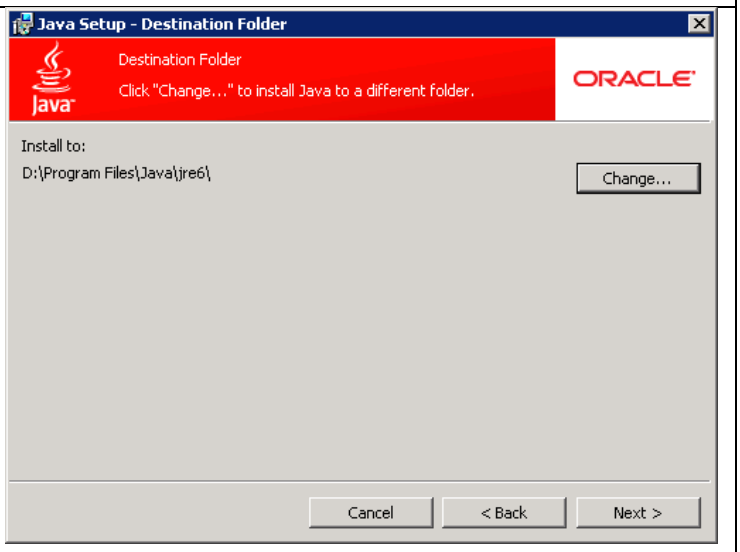
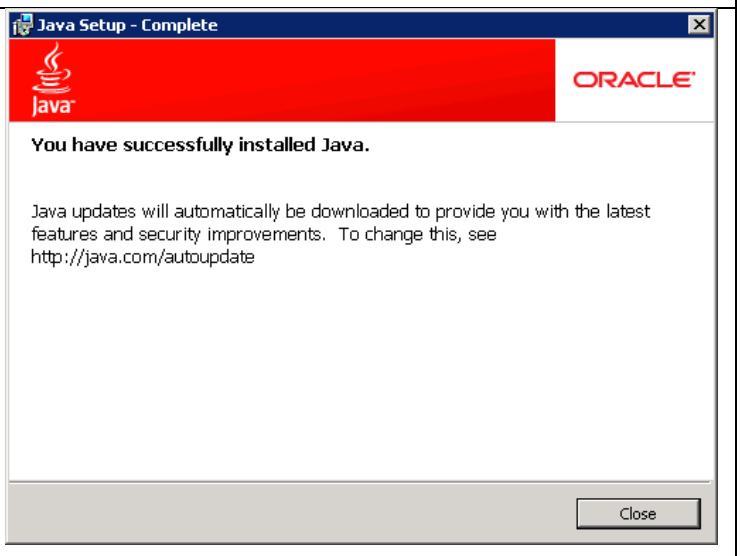
357

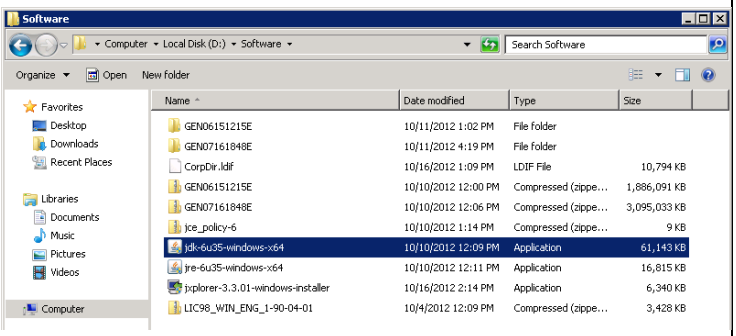
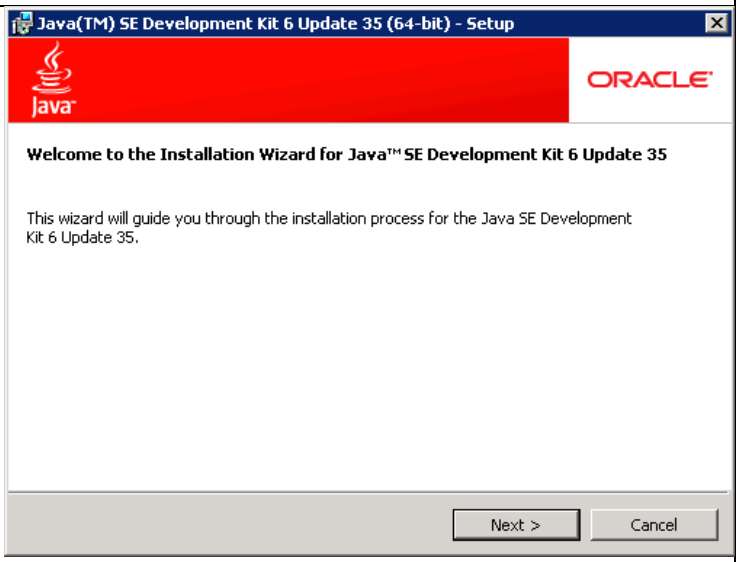
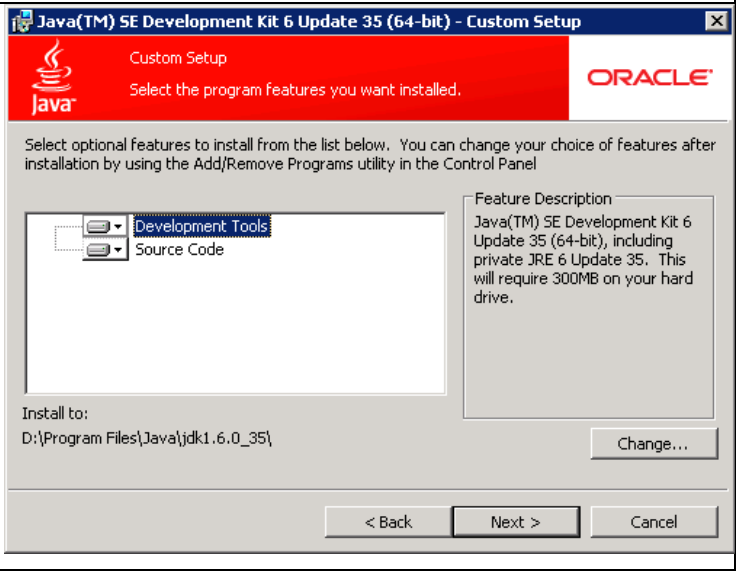
Desde el JXplorer Haga clic en la pestaña LDIF en la parte superior y seleccione Exportar árbol completo	
Ponga la información DN como se muestra en la pantalla y haga clic en Aceptar	
Esta pantalla le pedirá que guarde el archivo LDIF con el nombre CorpDir.ldif	

358

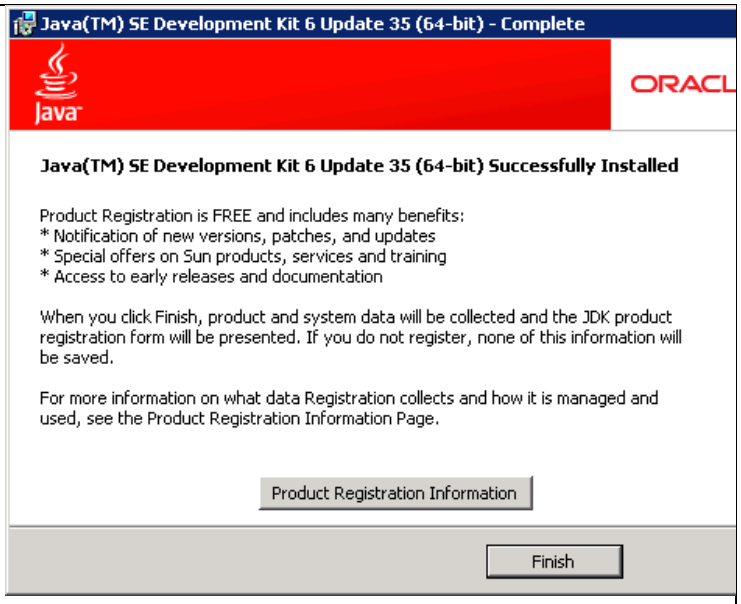
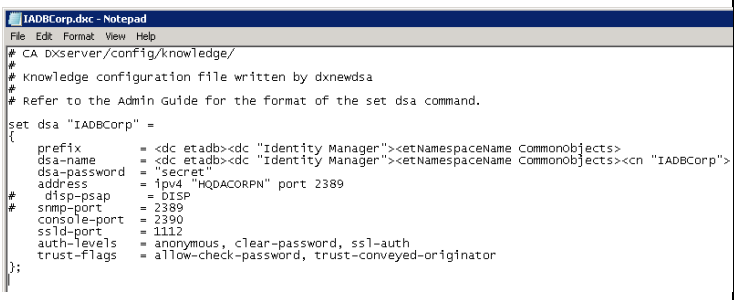
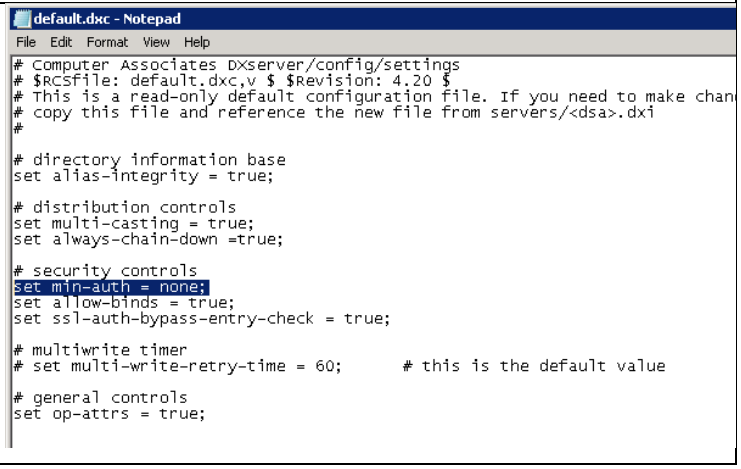
Esta pantalla muestra el archivo LDIF de ser salvos.	
Detenga el servidor de DX y en el siguiente paso podemos cargar las entradas db utilizando el comando dxloaddb que utiliza el archivo LDIF creado previamente .	
Comience TODAS dxserver / s con el comando mostrado " dxserver empezar "	
Vaya a la ubicación del directorio de software se muestra y ejecutar el archivo jre- 6u35 - windows- x64 para instalar JRE	

359

En esta pantalla de bienvenida haga clic en " Instalar"	
Seleccione la carpeta de destino JAVA como d: \ Archivos de programa \ Java \ jre6 (Si no es igual que el anterior botón de cambio de clic y escriba la ruta correcta . Haga clic en Siguiente"	
Exitosa pantalla de finalización de la instalación confirmará la instalación. Haga clic en el botón de cierre .	

Para instalar JDK , vaya a la ubicación del directorio de software y ejecutar el archivo de aplicación jdk - 6u35 -windows- x64	
JDK Bienvenido instalación aparecerá la pantalla, Haga clic en Siguiente"	
Seleccione las herramientas de implementación disponen de instalar y haga clic en Siguiente	

361

Esta pantalla mostrará la información de registro del producto , haga clic en el botón de meta.	
Abra el archivo IADBCorp.dxc , y asegúrese de que parece el mismo que en esta pantalla , y quitar el anonimato de la línea auth -niveles en la parte inferior .	
	REMOVE ANONYMOUS AFTER FINALIZING
El archivo default.dxc , reemplace 'none' con la contraseña en el 'set min -auth "línea como se destaca .	

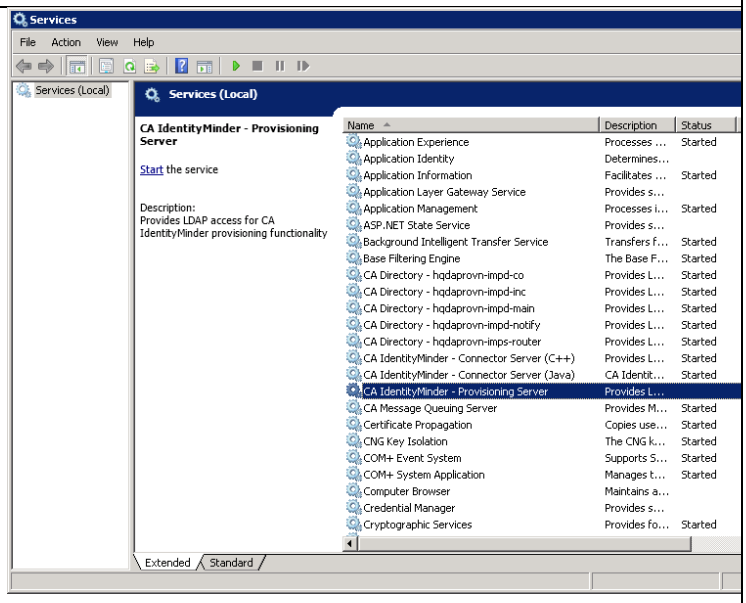
2.1.8 Migracion de directorio de datos de abastecimiento

362

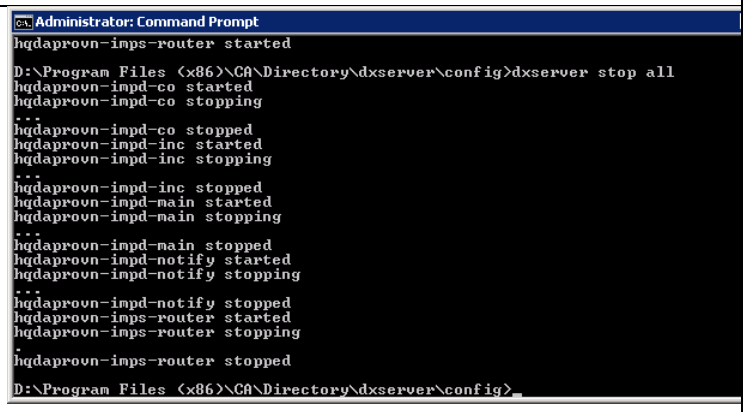
2.1.9 Migracion de directorio de datos de abastecimiento

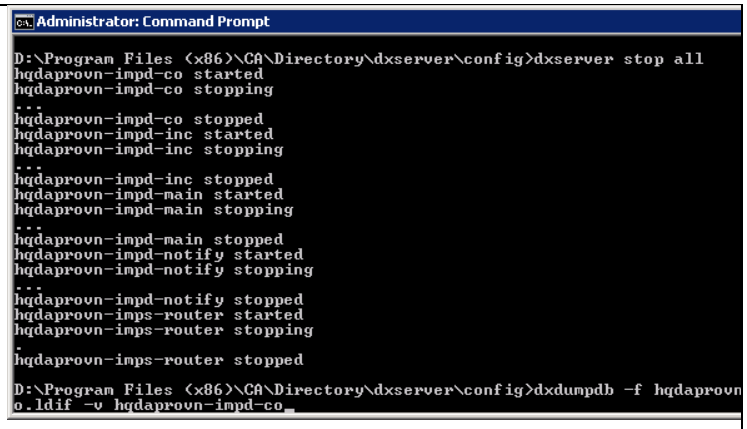
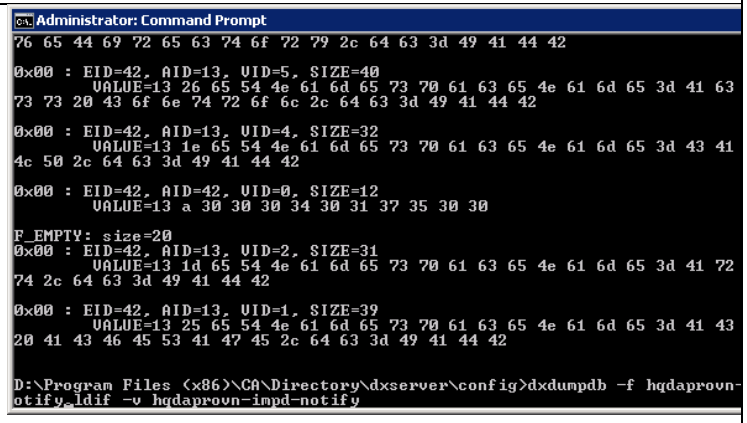
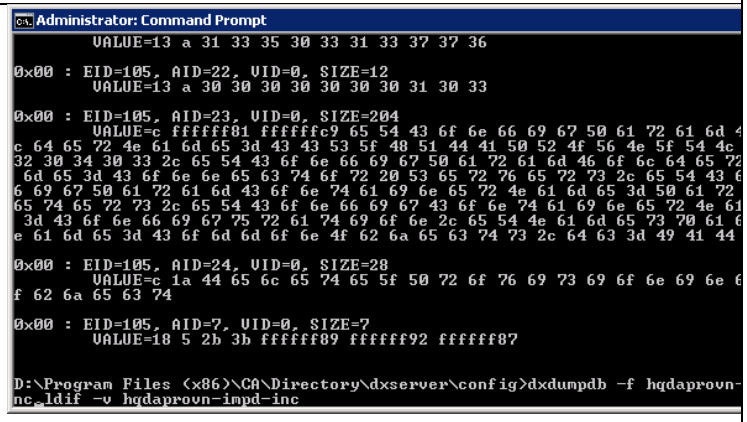
El Antiguo prov servidor ejecute el comando dxdumpdb .

Deje de Prov . Server de la herramienta de los servicios como se destaca en la pantalla. (Para detener / iniciar , haga clic derecho sobre el nombre del servicio y seleccione stop / start)

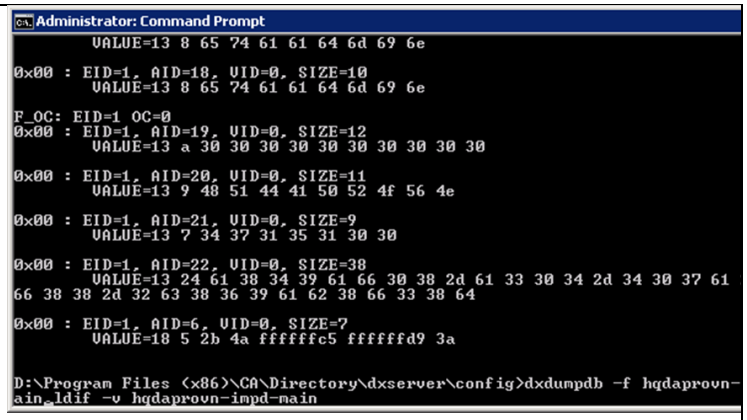
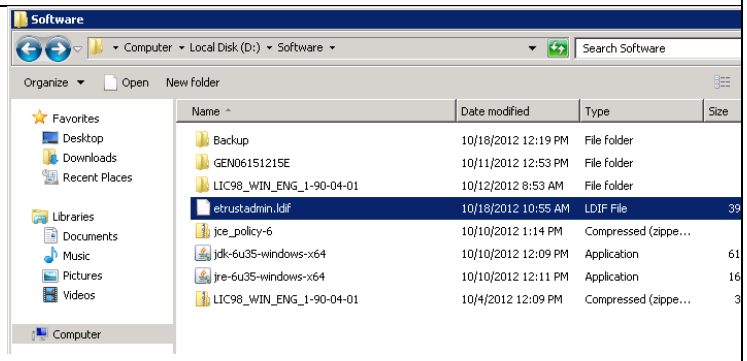
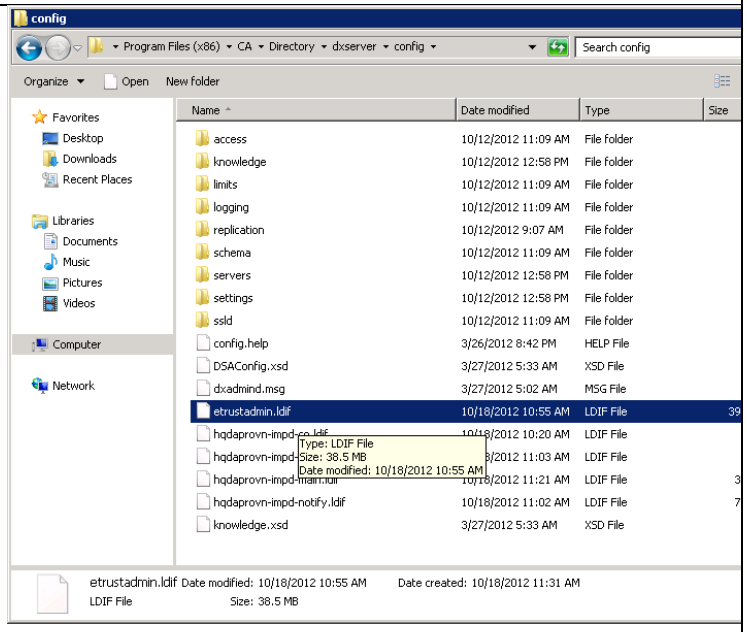


Realizar la siguiente en el nuevo servidor de aprovisionamiento. Los pasos ayudan a una copia de seguridad del contenido del directorio de aprovisionamiento antes de la importación de datos desde el directorio de edad

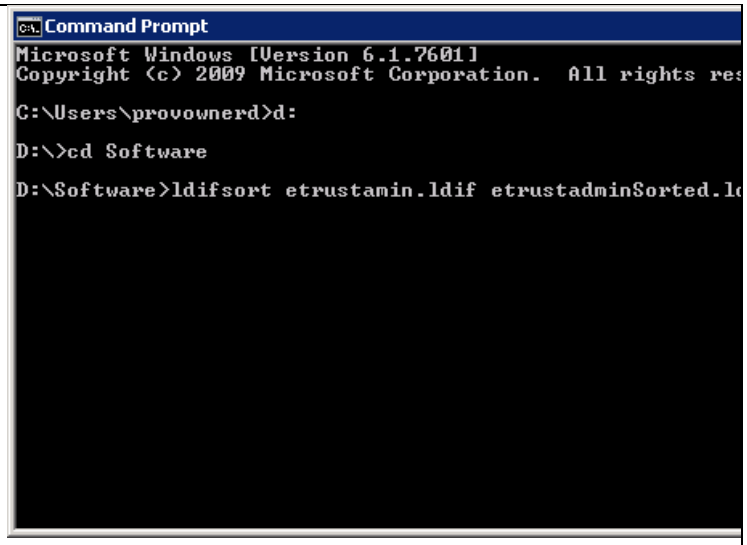
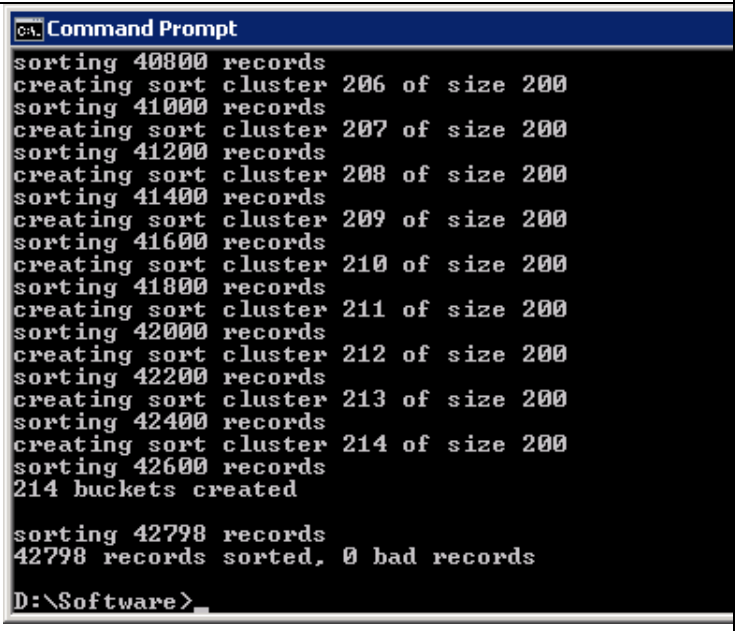
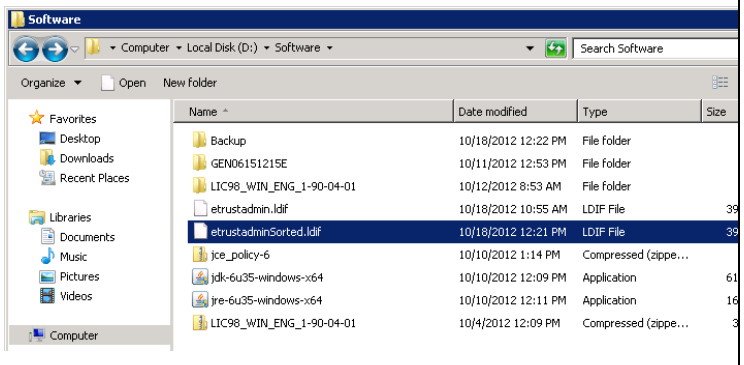


Deje de dxservers como se muestra en la línea de comandos .	
Ejecute el comando dxdumpdb para el archivo ' hqdaprovn - IMPD - co.ldif ' con los parámetros que se muestran en la última línea de la pantalla.	
Ejecute el comando dxdumpdb para el archivo ' hqdaprovn - IMPD - inc.ldif ' con los parámetros que se muestran en la última línea de la pantalla.	

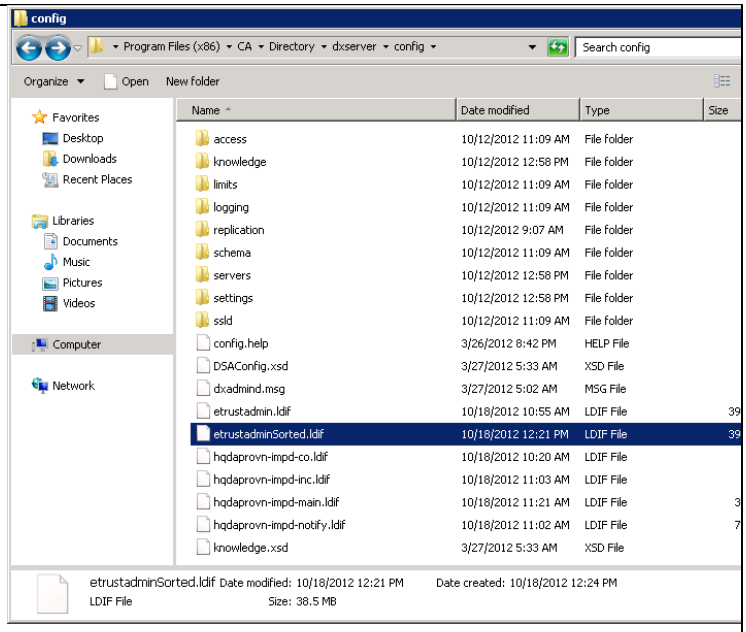
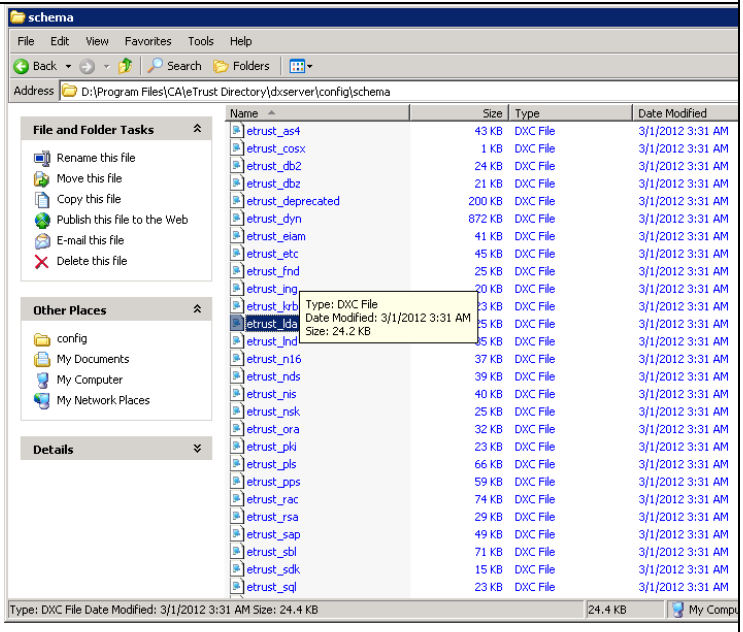
364

Ejecute el comando dxdumpdb para el archivo ' hqdaprovn - IMPD - main.ldif ' con los parámetros que se muestran en la última línea de la pantalla.	
Ir a la ubicación del directorio de software y copiar el archivo etustadmin.ldif	
Pegue el mismo archivo en el directorio de configuración como se muestra en la pantalla.	

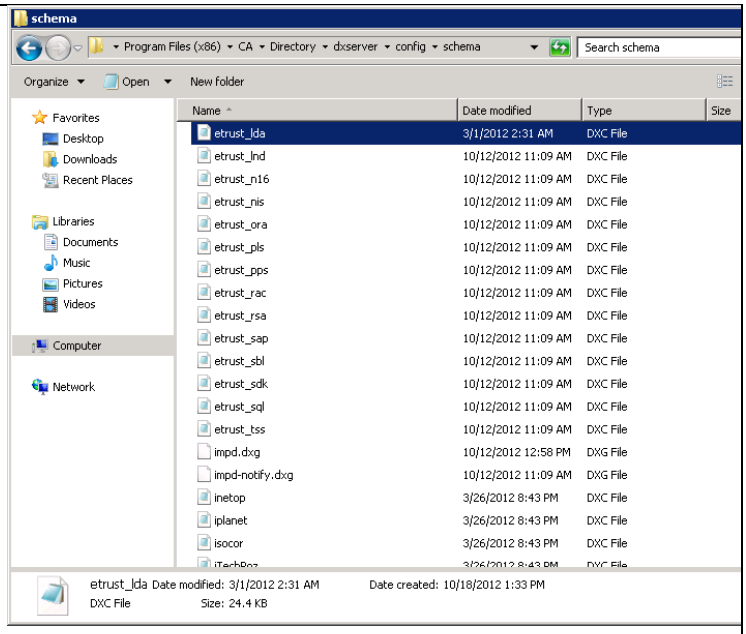
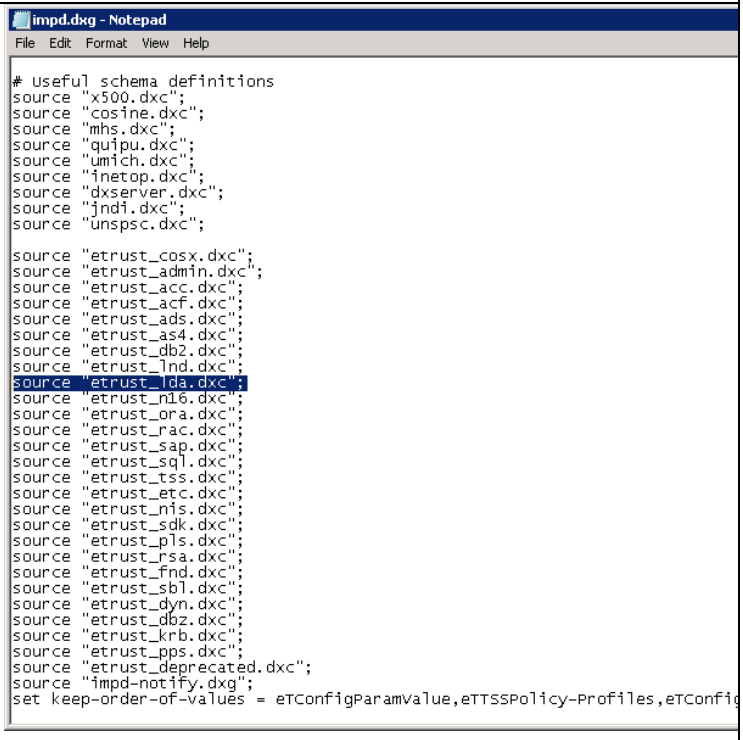
365

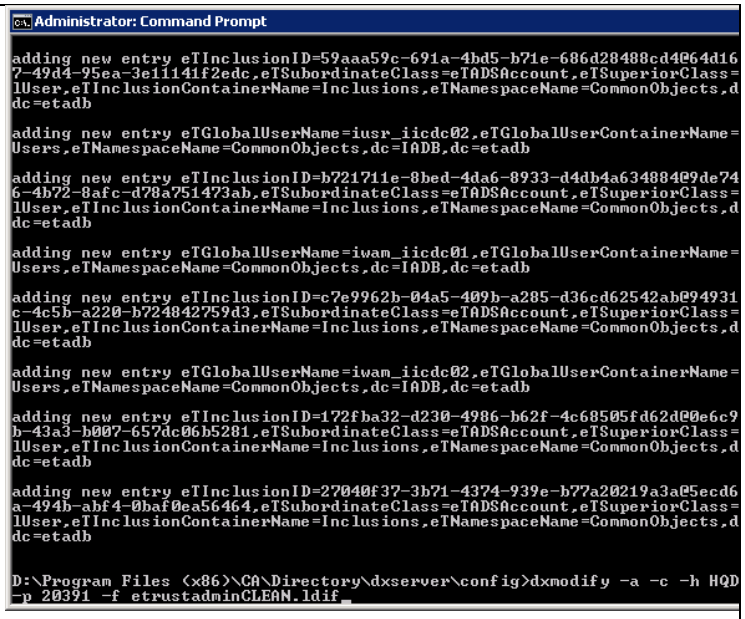
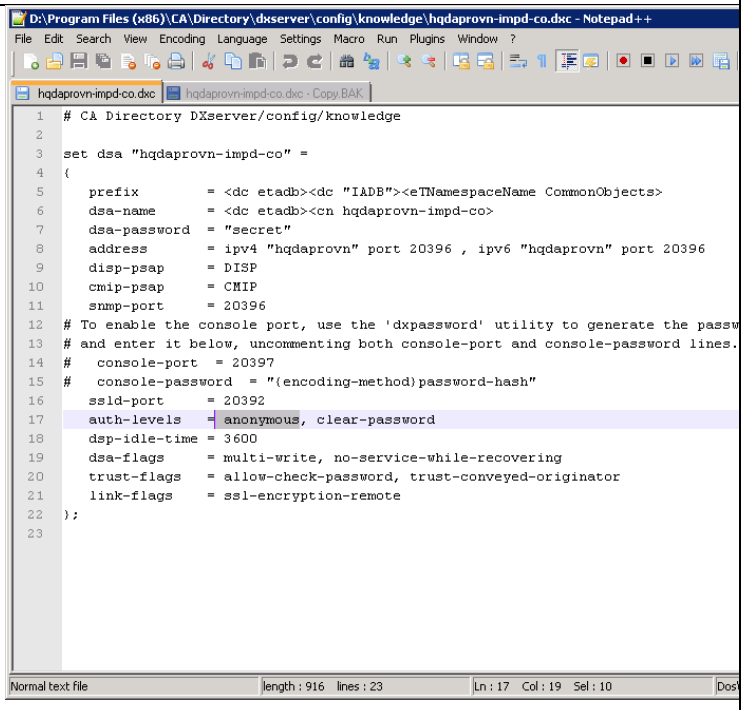
Ir al símbolo del sistema , y cd d: \ software .	
Será comprobar que no existen registros malos y si todos los registros son buenos , debería ver '0 ' malos registros al final.	
Ir a la ubicación del directorio de software y copiar el archivo etustadminSorted.ldif	

366

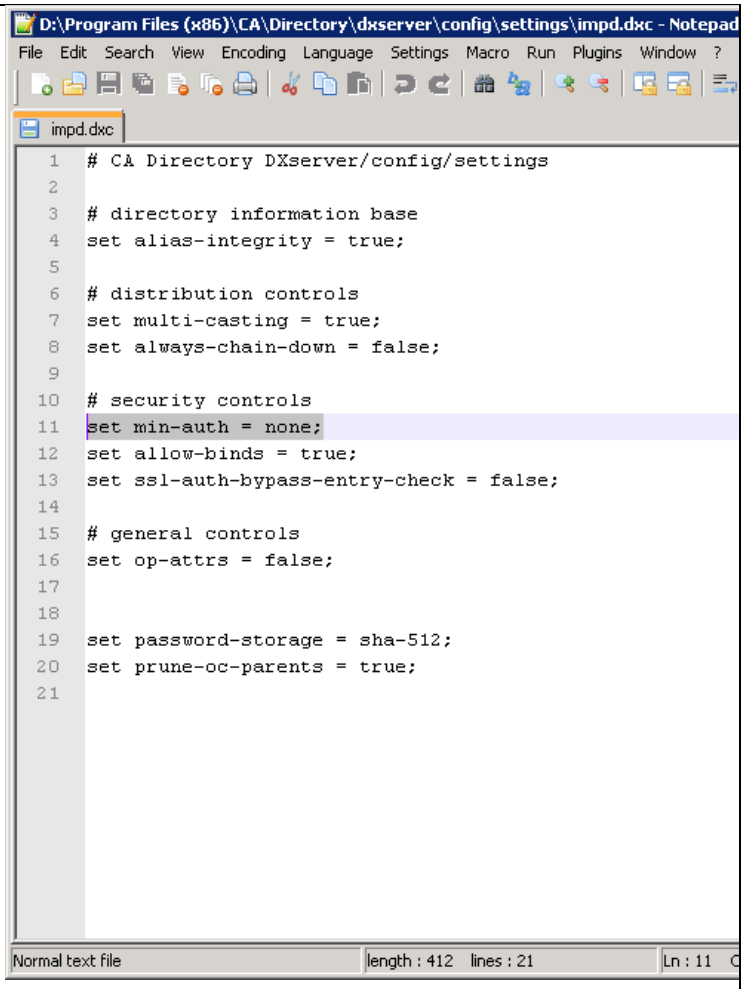
Pegue el mismo archivo en el directorio de configuración como se muestra en la pantalla.	
Archivo etrust_lda COPIA de viejo a nuevo sistema de directorio de esquema como se muestra en la pantalla.	

367

Pegue etrust_lda archivo para el nuevo sistema .	
Verifique que el archivo impd.dxg tiene entrada para etrust_lda.dxc (como se destaca en la pantalla) .	

Ejecutar comando DXModify utilizando los parámetros que se muestran en la parte inferior de la pantalla. Se añadirá nuevas entradas , como se muestra en la pantalla de arriba.	
Retire el anonimato después de finalizar (como se muestra en la pantalla) .	

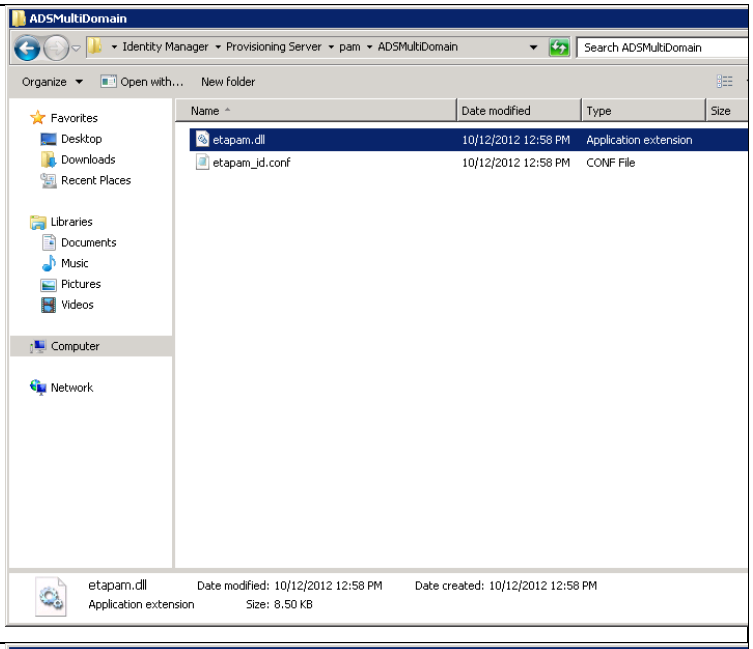
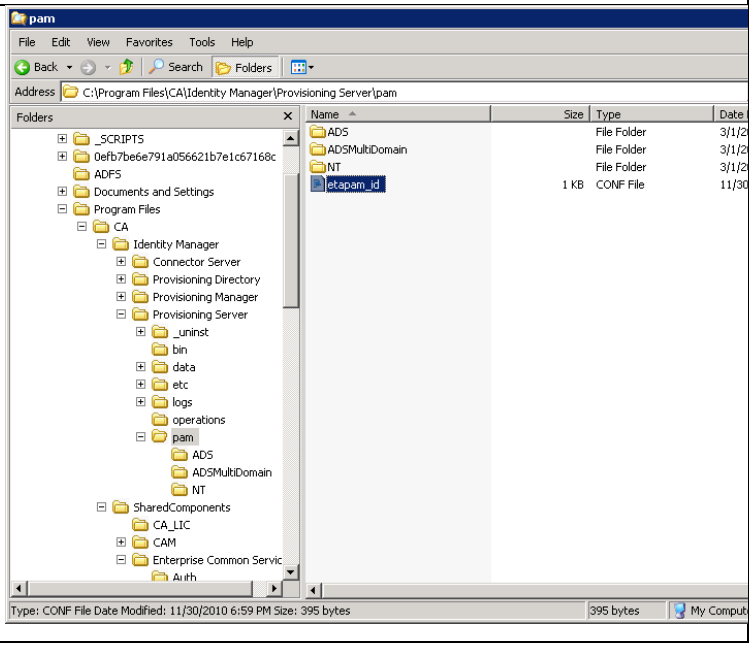
369

Compruebe la configuración impd.dxc	

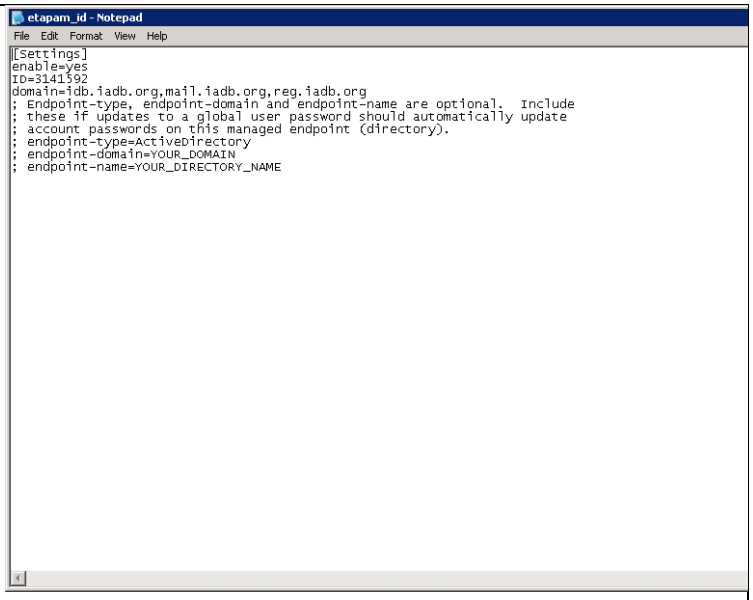
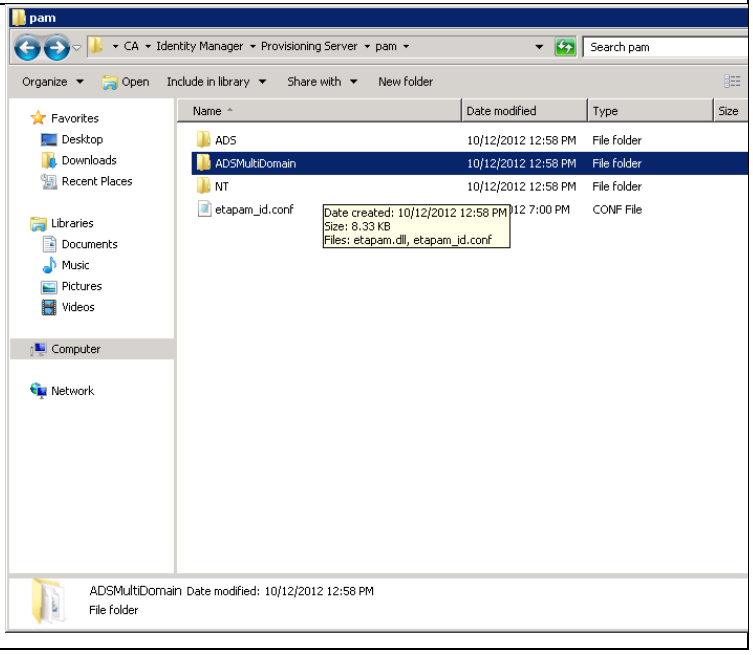
2.1.10 PAM y personalizacion

PAM y personalización

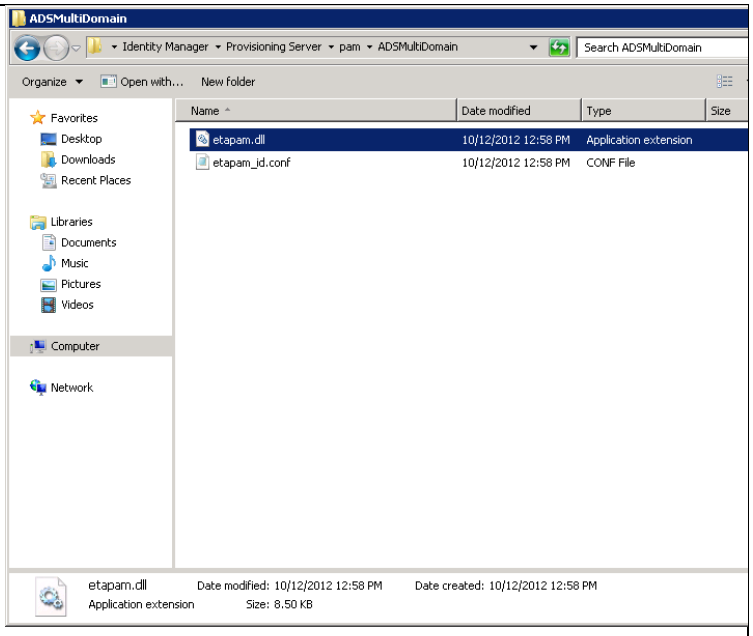
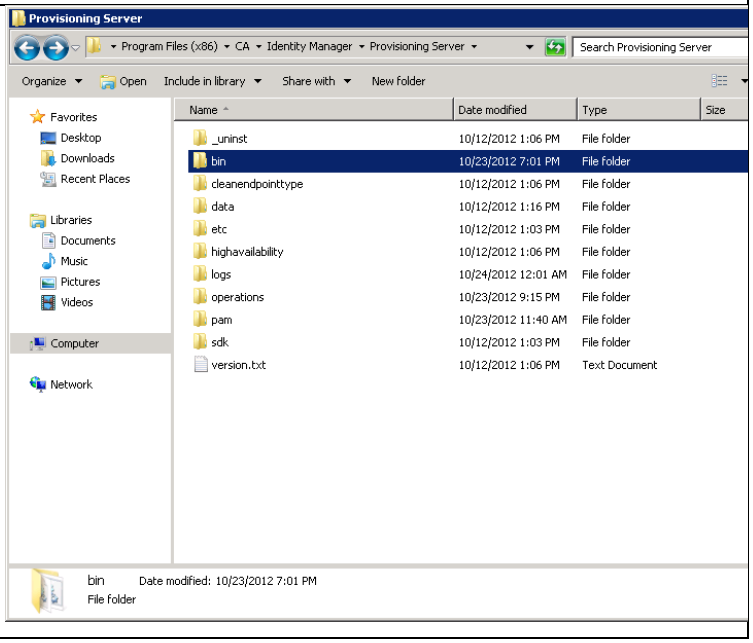
370

Ir a la carpeta ADSMultiDomain y copiar el eta_pam_id a la raíz de la carpeta pam	
Abra el archivo de configuración ' eta_pam_id ' .	

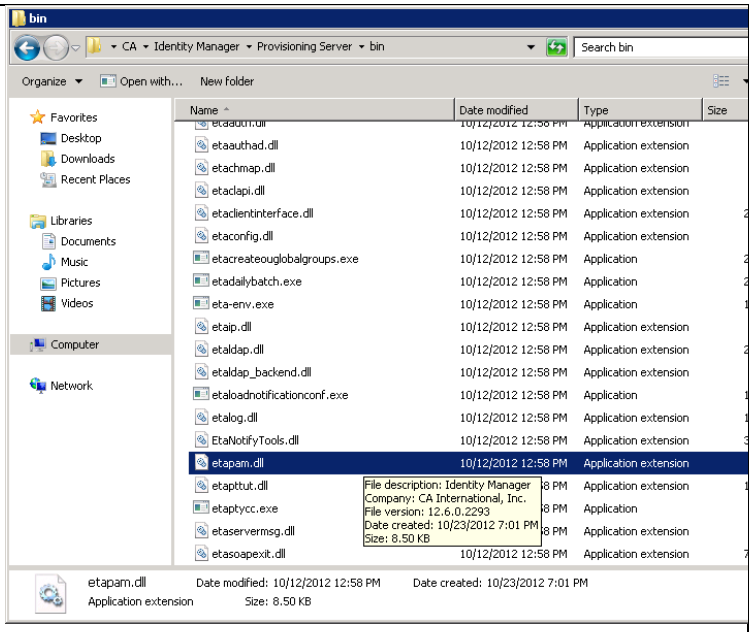
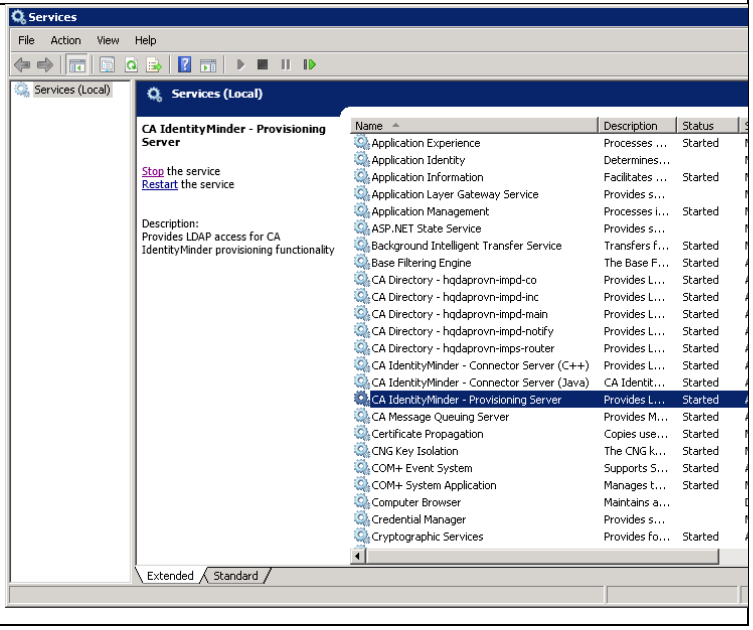
371

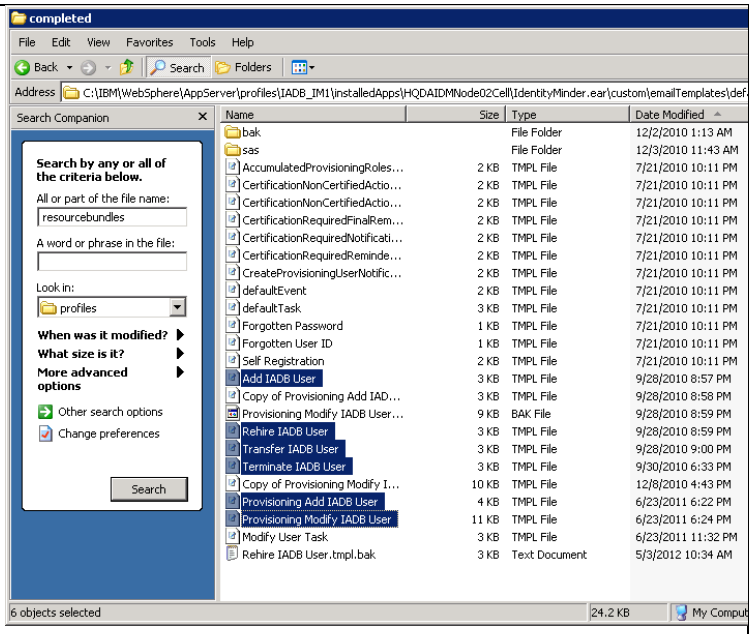
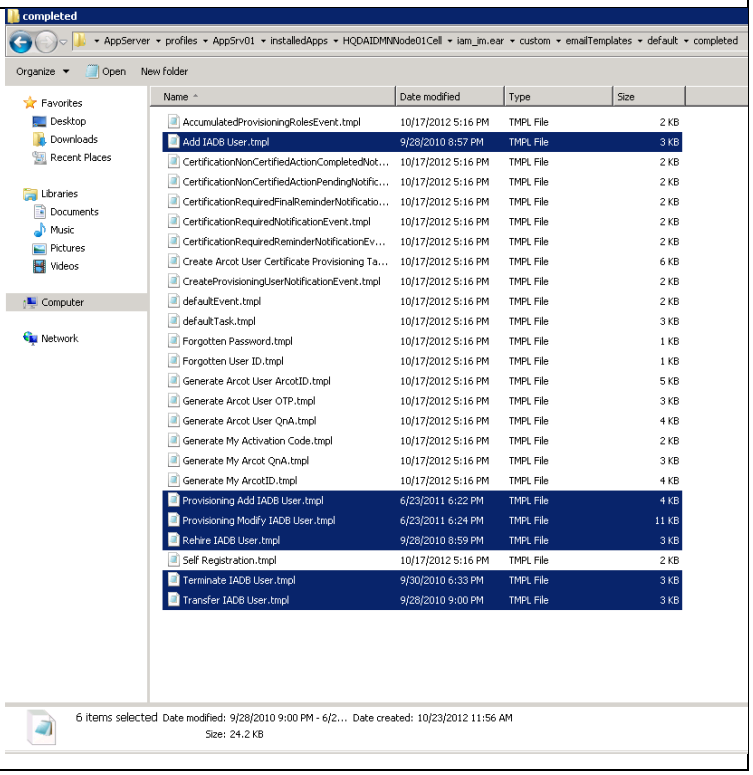
Verifique el contenido de los archivos son similares a la captura de pantalla .	
Entra en el directorio ADSMultiDomain .	

372

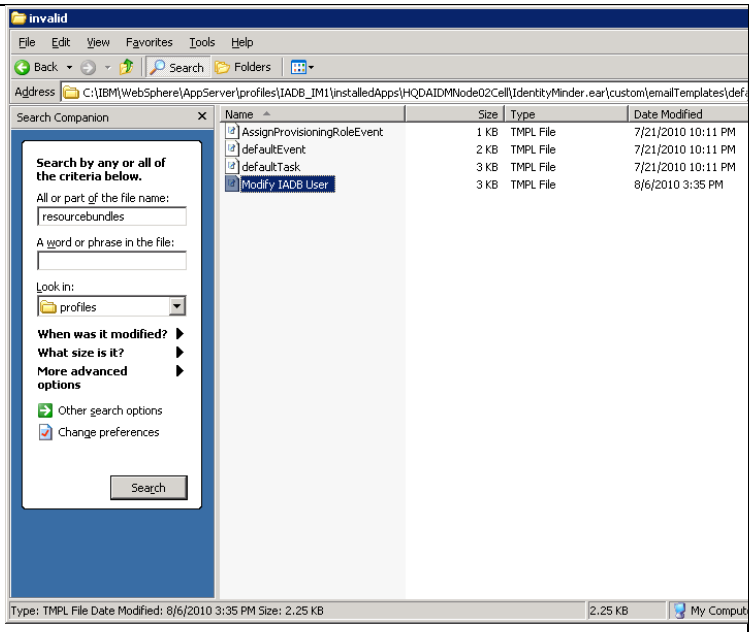
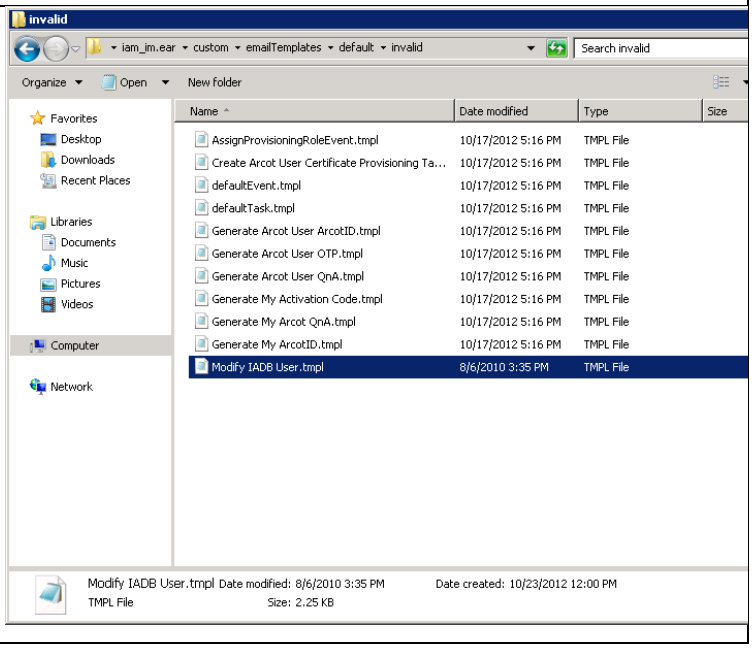
Copie el archivo etapam_id.conf del directorio pam (un nivel por encima) de aquí . Copie el archivo etapam.dll desde aquí.	
Ir a la Prov . Directorio bin del servidor , como se muestra en la pantalla	

373

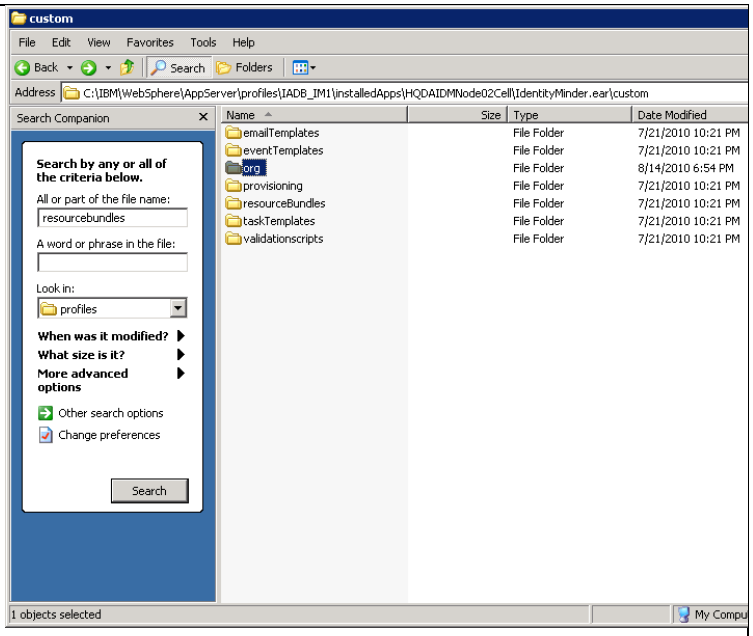
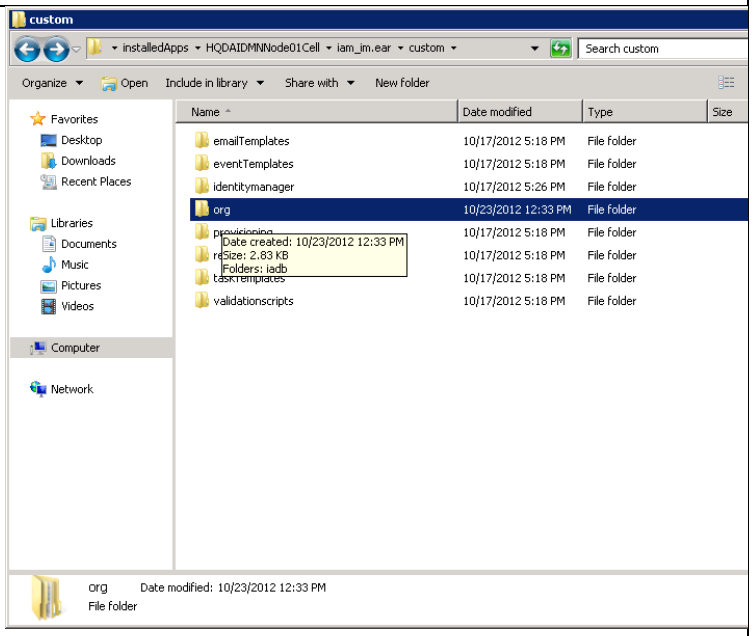
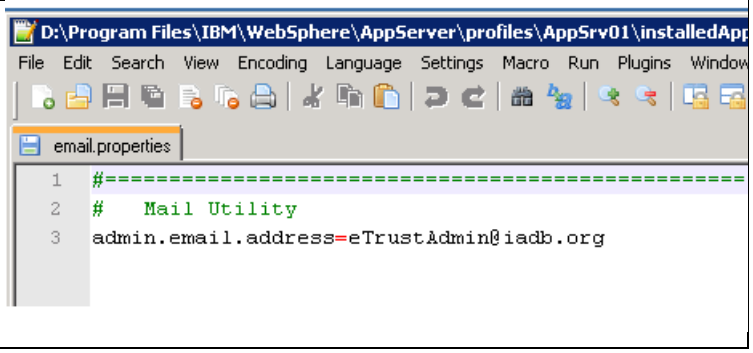
Pegue etapam.dll archivo aquí .	
Reinicie el servidor de aprovisionamiento	

En la vieja copia del servidor de aprovisionamiento en los plantillas de correo electrónico personalizados resaltado en la pantalla	
Pegarlos en el mismo directorio en el nuevo servidor de aprovisionamiento	

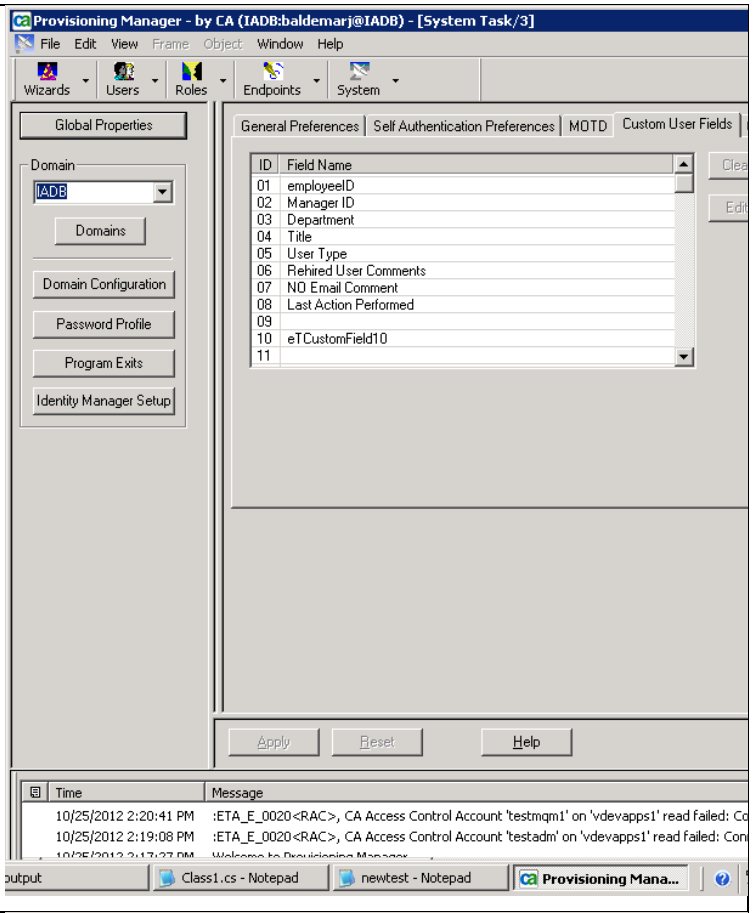
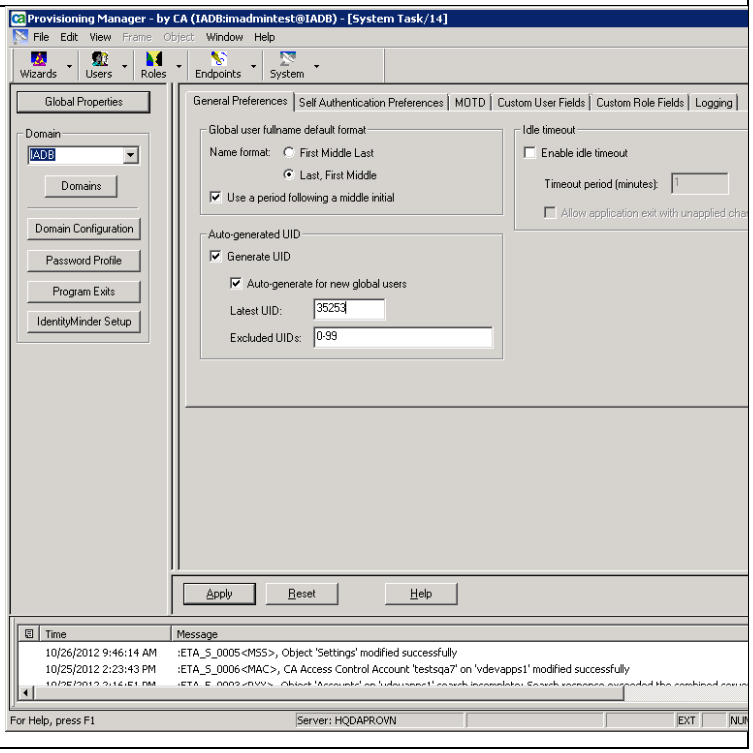
375

En el servidor de aprovisionamiento de edad vaya al directorio mostrado y copiar la plantilla modificar usuario BID	
Coloque el usuario Modificar BID en el directorio no válido en virtud de la costumbre	

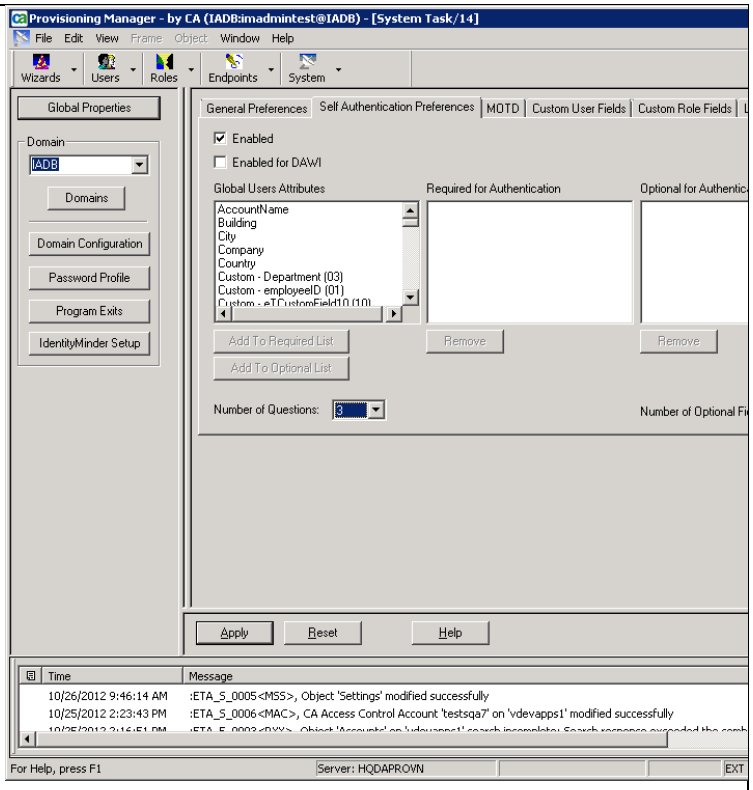
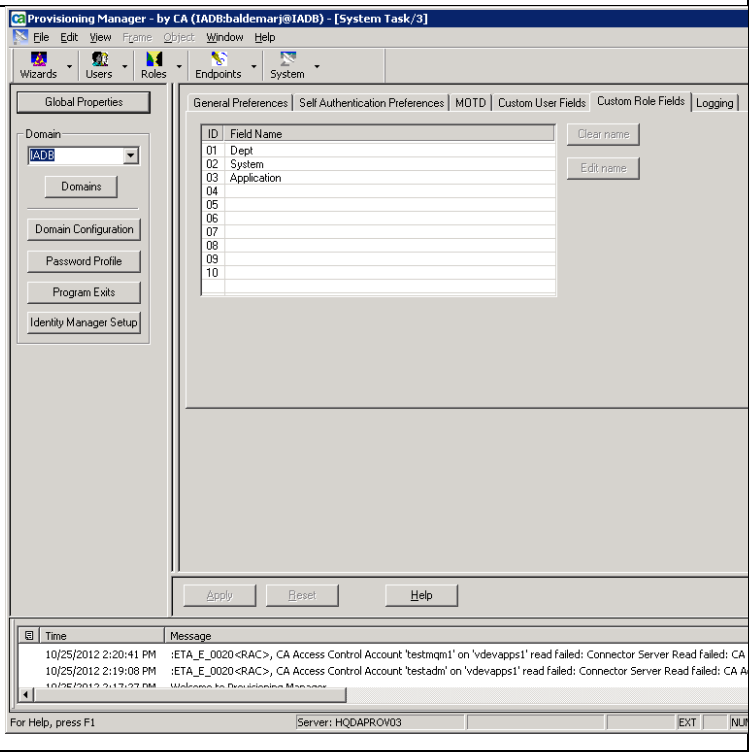
376

Copiar sobre la carpeta org del servidor antiguo	
Pegar la carpeta org en la trayectoria equivalente en el nuevo servidor de aprovisionamiento	
Compruebe que el archivo email.properties se establece . D: \ Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\HQDAIDMNNode01Cell\iam_im.ear\config\com\netegrity\config	

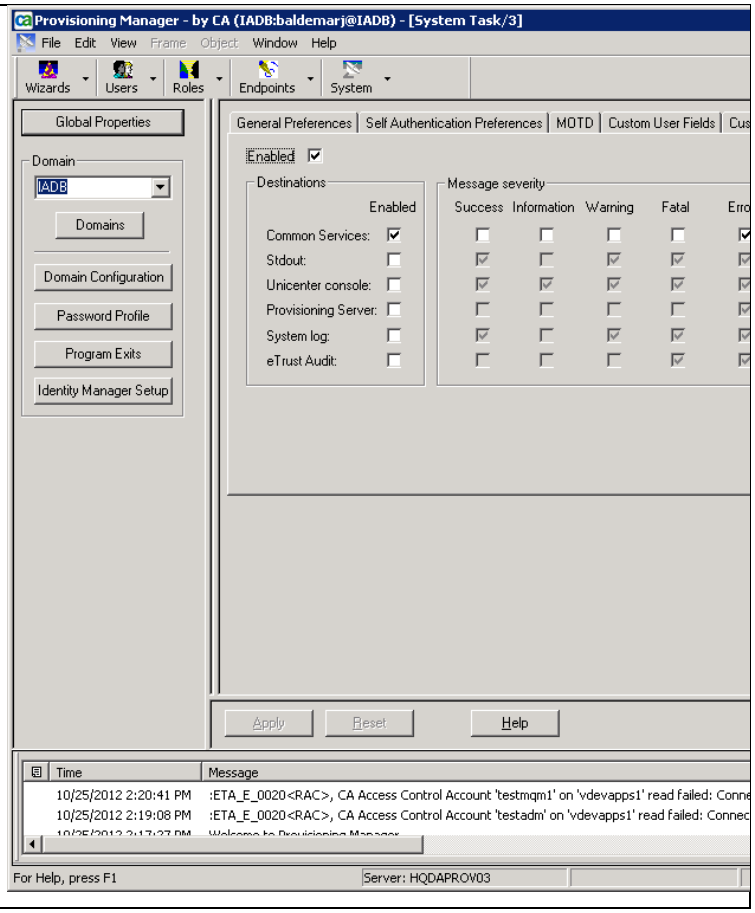
377

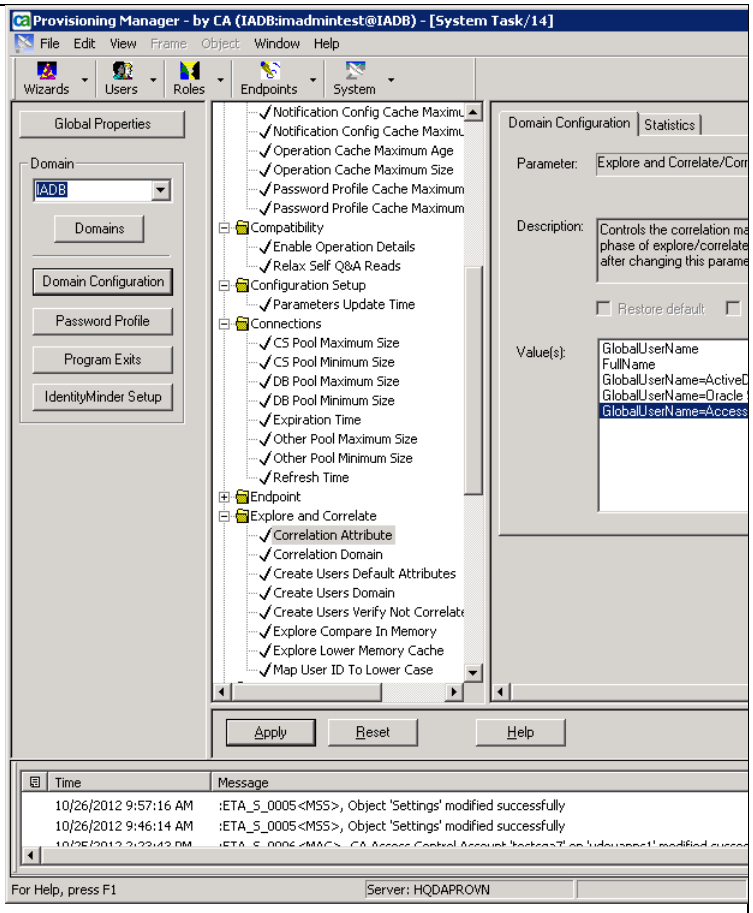
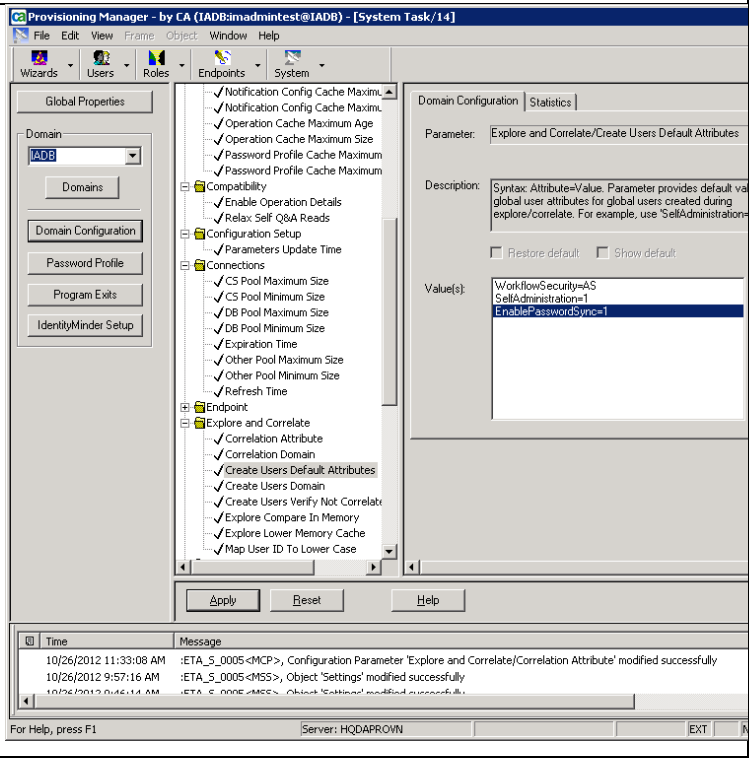
Establezca el campo de usuario personalizada en el gestor de aprovisionamiento	
Establezca la pestaña general preferencias en el gestor de aprovisionamiento como se muestra en la captura de pantalla	

378

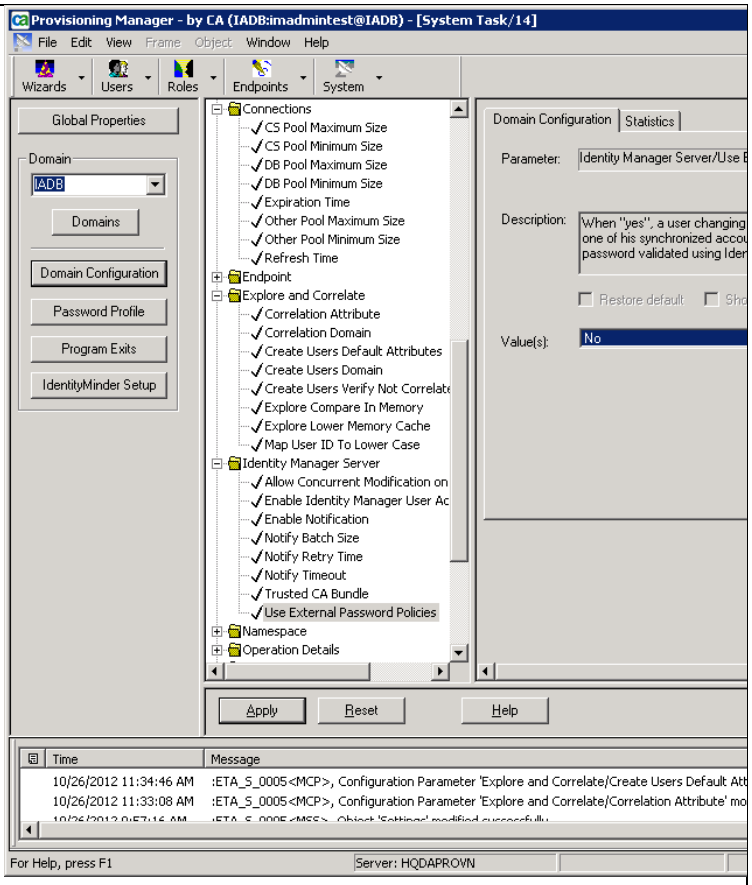
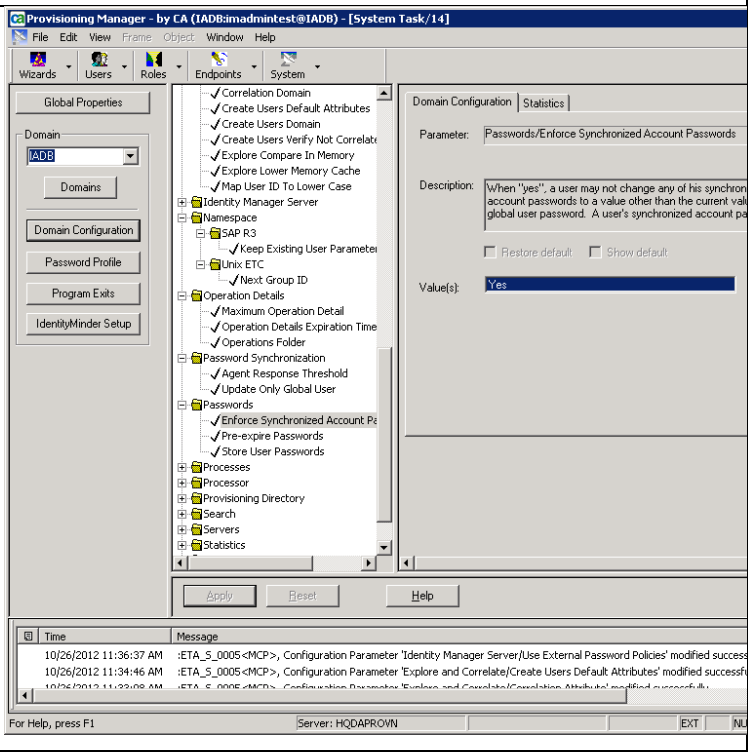
Compruebe el habilitada en las preferencias de autenticación por cuenta y establecer el número de preguntas para 3	
Introduzca los campos de roles personalizados , como se muestra	

379

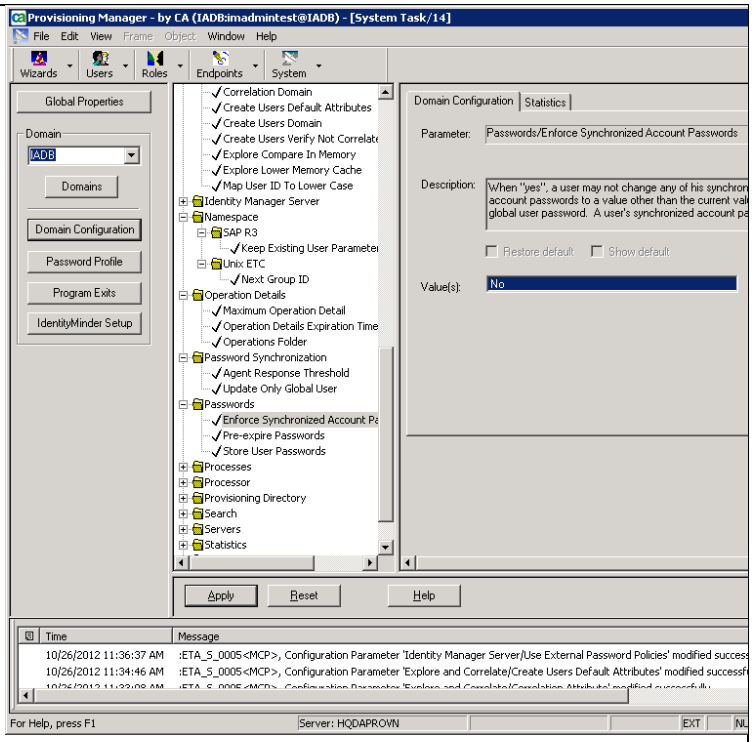
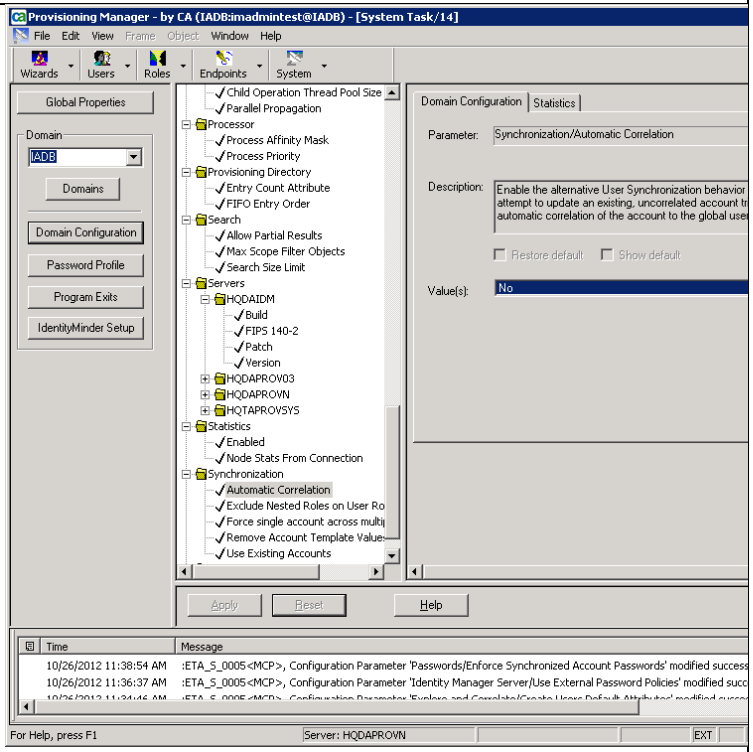
Compruebe permitido bajo la tala y seleccione las casillas que se muestran	

Añadir los atributos de correlación mostrados	
Agregue el crear usuarios atributos predeterminados	

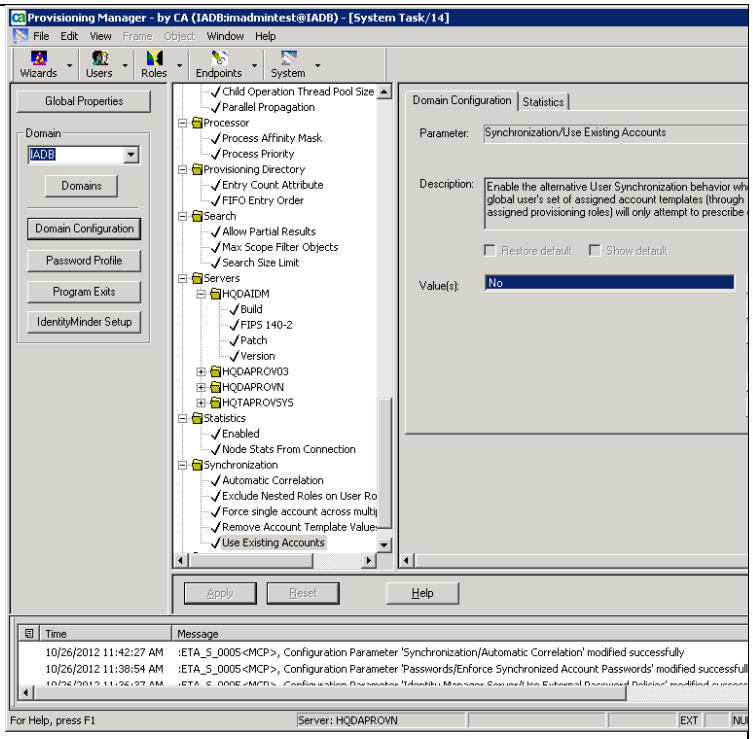
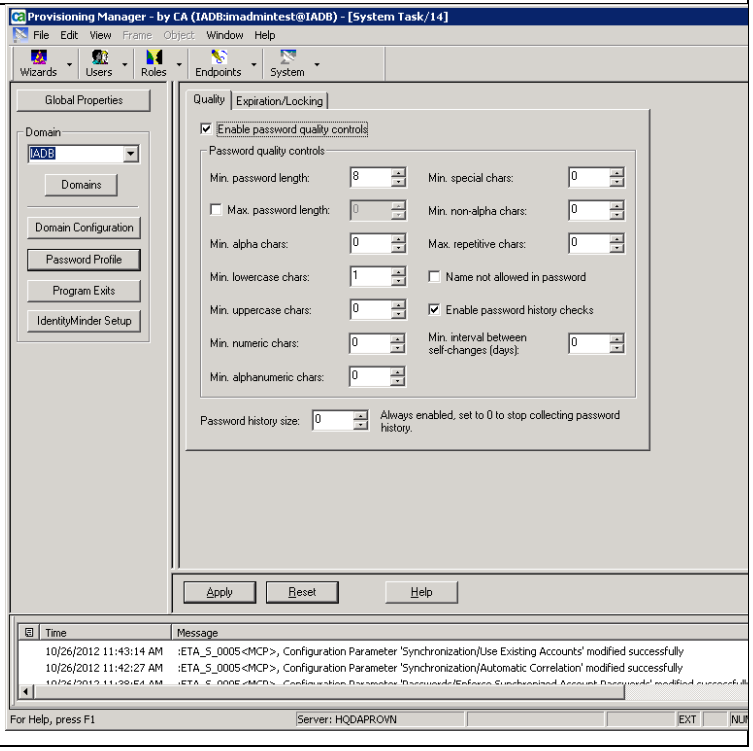
381

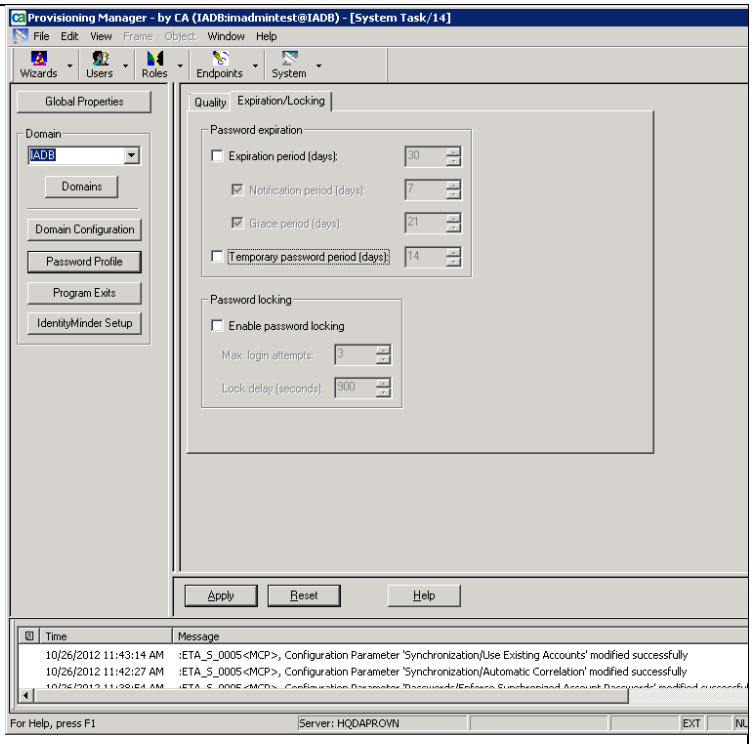
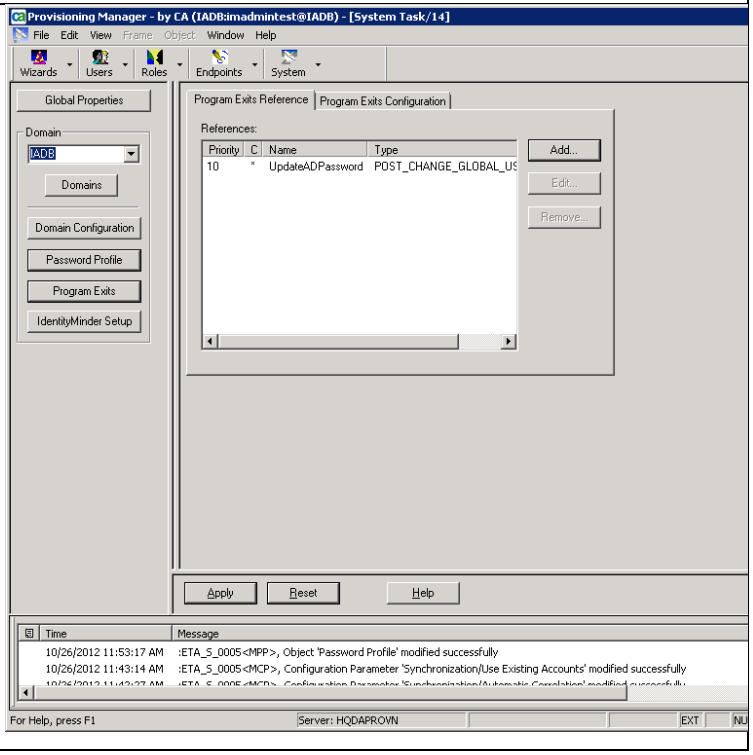
De Provisioning Manager- > IDM Servidor-> Contraseña uso externo políticas- > Valor de ajuste de "No" , como se muestra en la pantalla.	 From Provisioning manager->
De Provisioning Manager- > passwords > Contraseña cumplir sincronización de cuentas con contraseña > valor es ' Sí ' , como se muestra en la pantalla.	

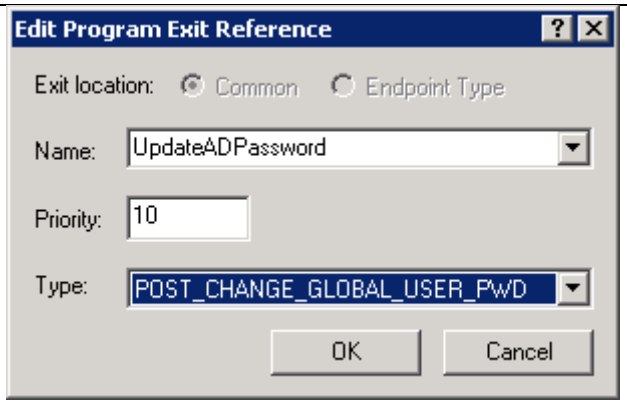
382

De Provisioning Manager- > passwords > Contraseña cumplir sincronización de cuentas con contraseña > Valor seleccionado como ' No' , como se muestra en la pantalla.	
De Provisioning Manager- > Synchronization- > Correlation- automático> Valor seleccionado como ' No' , como se muestra en la pantalla.	

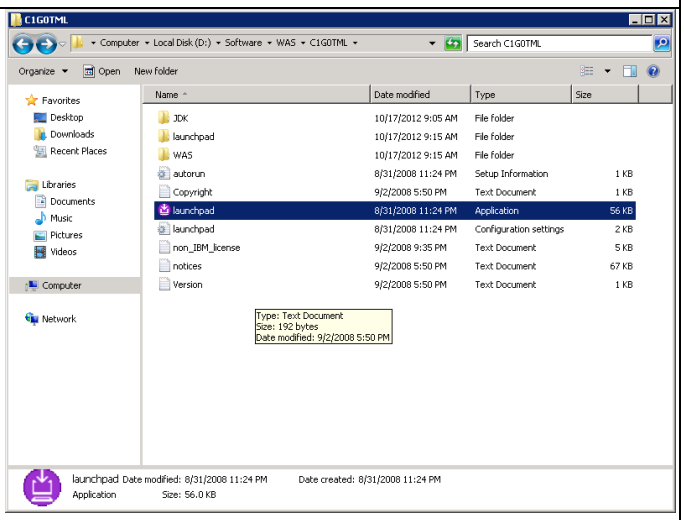
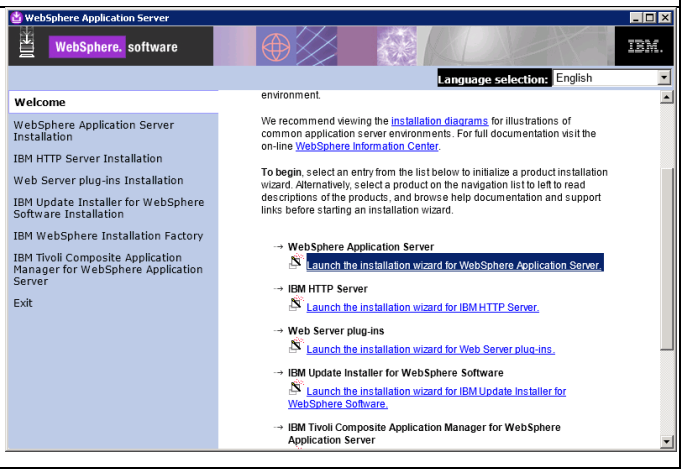
383

En Prov . Manager- > Synchronization- > Use Existing -Cuentas > Establecer valor como ' No' , como se muestra en la pantalla.	
En el perfil contraseña establecida la siguiente	

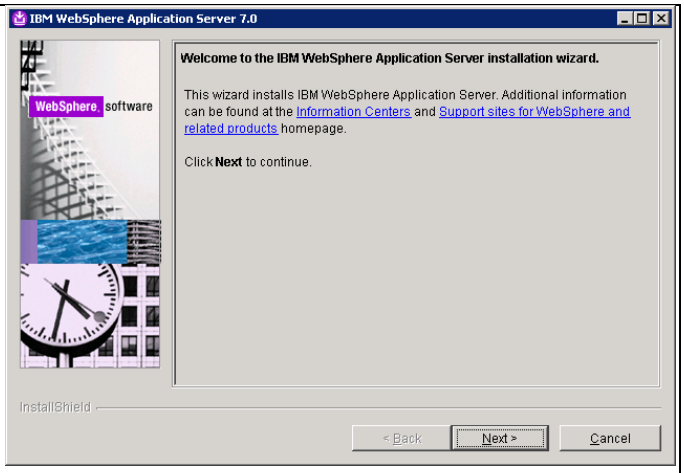
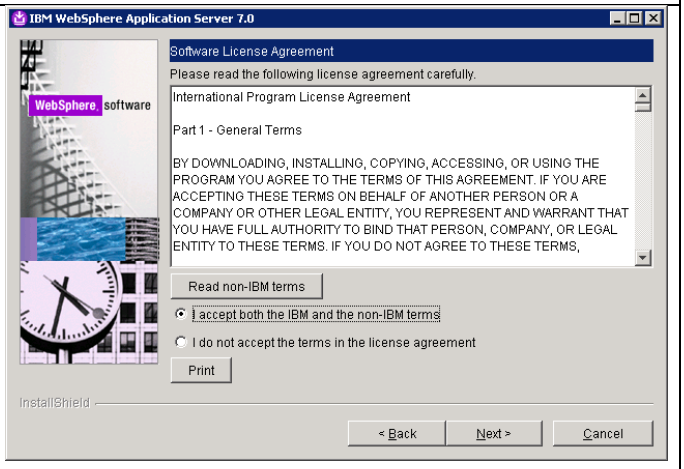
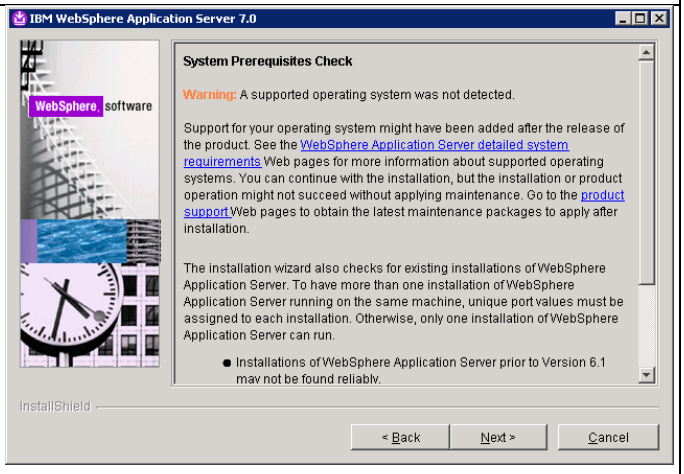
En el perfil de la contraseña en el / la lengüeta de fijación de caducidad fijado como se muestra en la captura de pantalla	
Haga clic en agregar programa se cierra y establecer la salida del programa (Agrega pantalla en la siguiente captura de pantalla)	

Pantalla de ajuste de salida del programa	

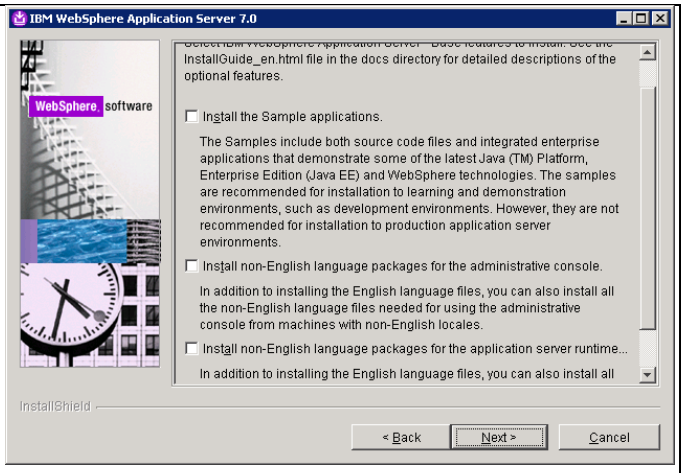
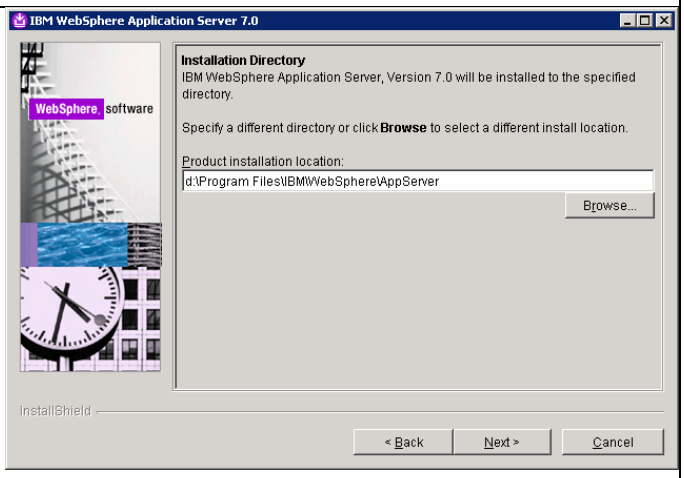
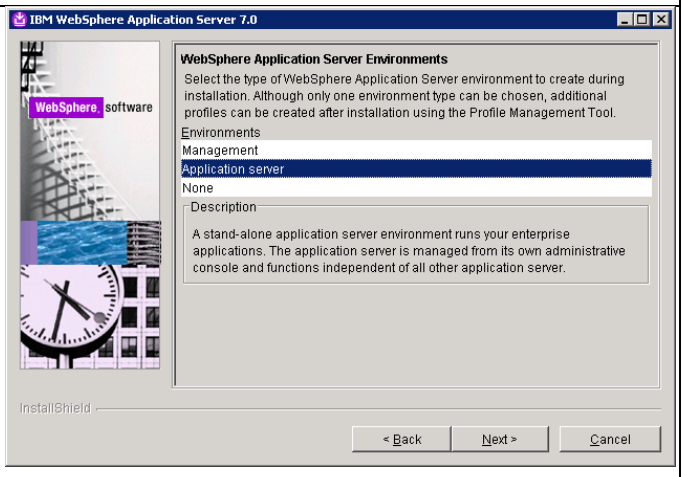
2.1.11 Instalacion de CA Identity Minder

INstalacion de CA Identity Manager	
Ejecute el Launchpad	
Seleccione Launc el asistente de instalación para el servidor de aplicaciones WebSphere	

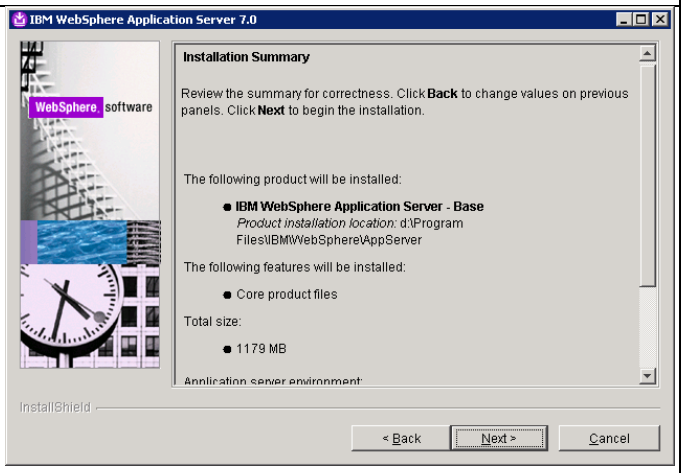
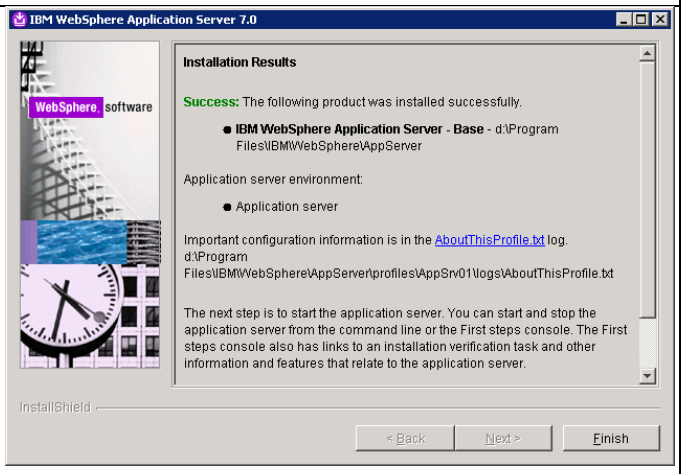
386

Haga clic en Siguiente	
Acepto las condiciones legales	
Haga clic en Siguiente	

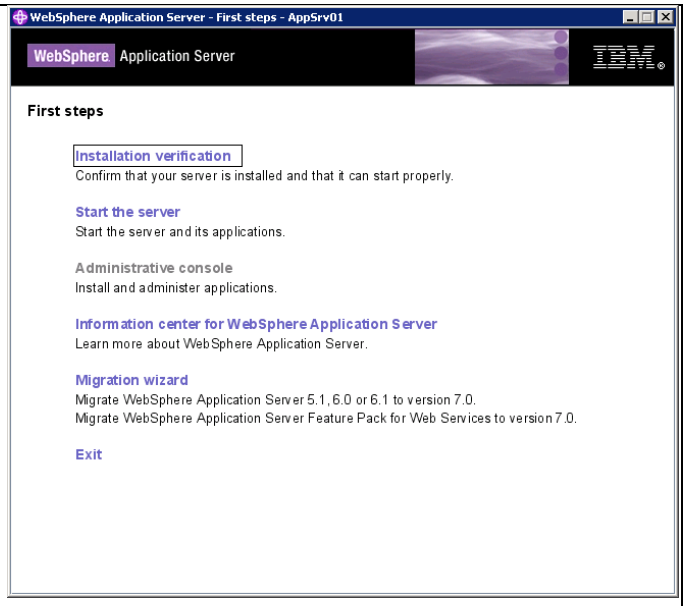
387

Mantenga todo sin control y haga clic en Siguiente	
Establezca la ruta de instalación	
Seleccione Servidor de aplicaciones	

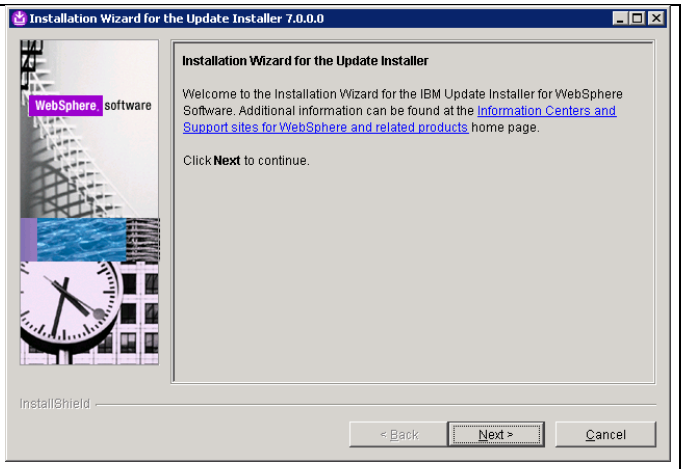
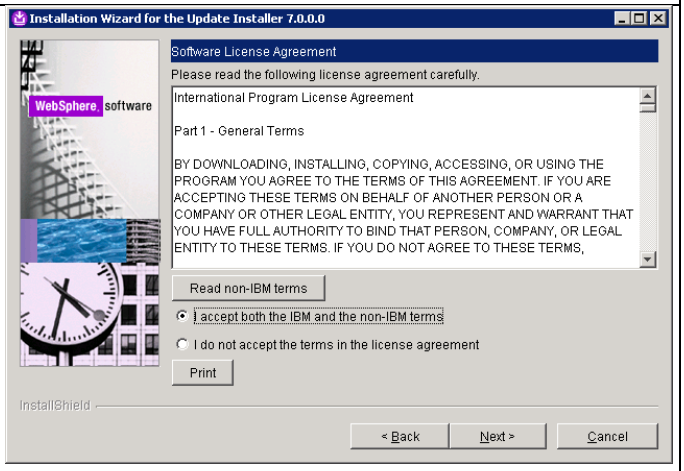
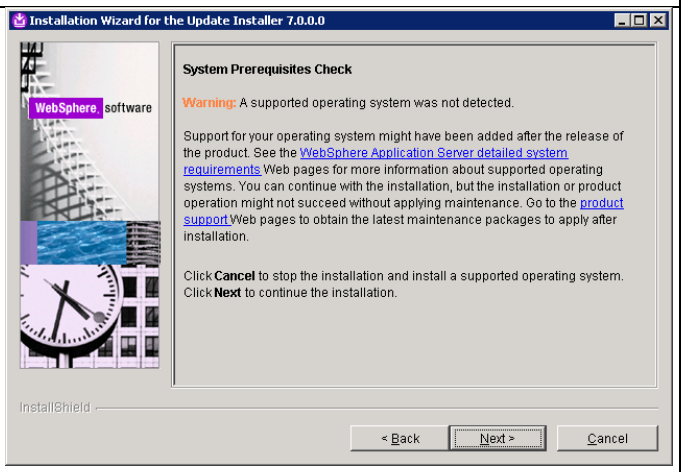
388

Desactive la opción Habilitar la seguridad administrativa . Se establecerá más adelante en la consola WAS	
Revise el resumen de la instalación y haga clic en Siguiente	
Después de la instalación, haga clic finist	

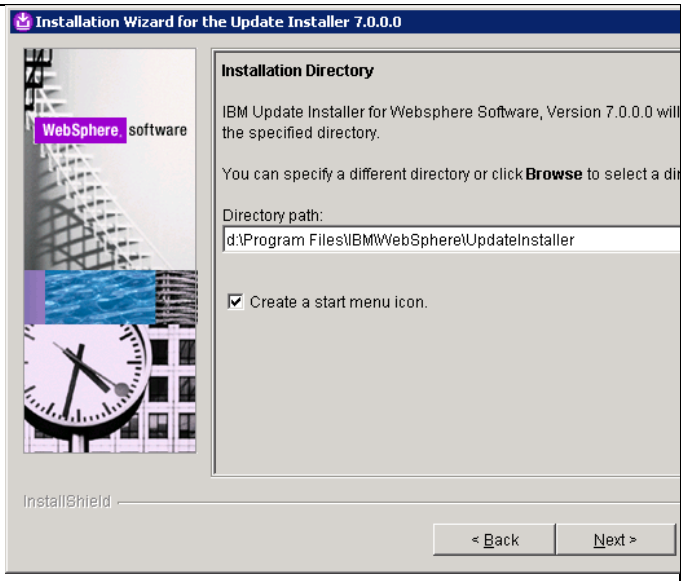
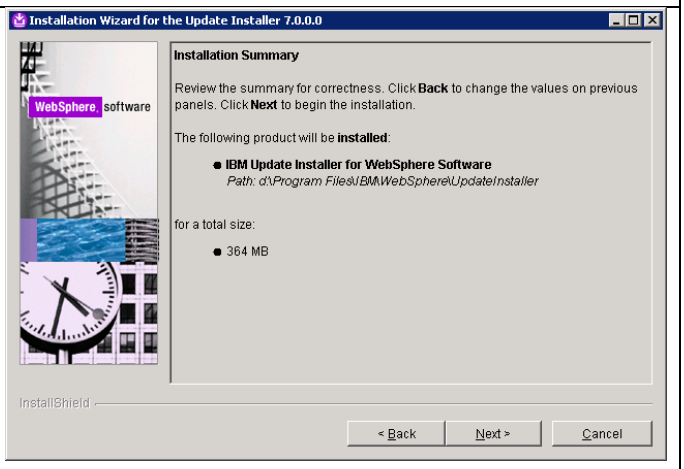
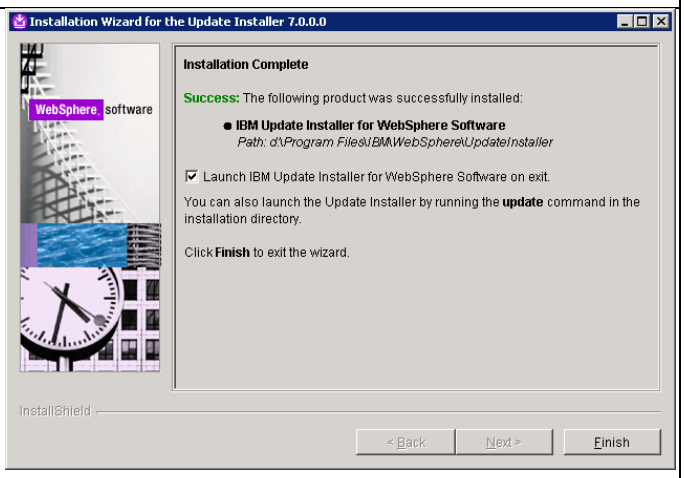
389

En la pantalla emergente , haga clic en Verificación de la instalación	
Revise la pantalla de verificación de la instalación	
En el Área de ejecución , haga clic en el enlace para instalar la instalación de la actualización	

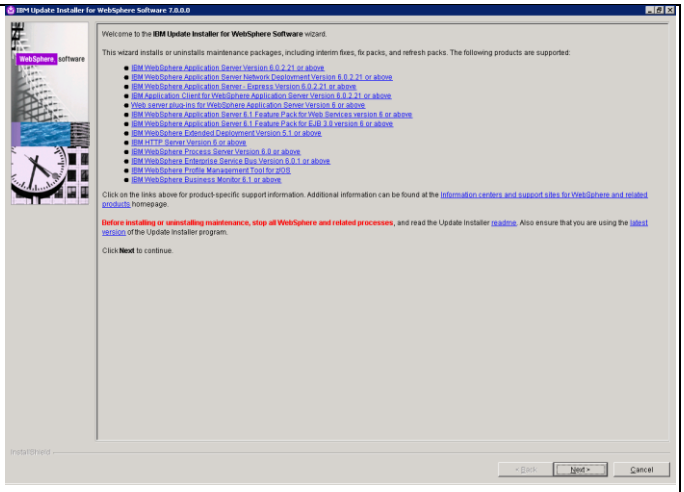
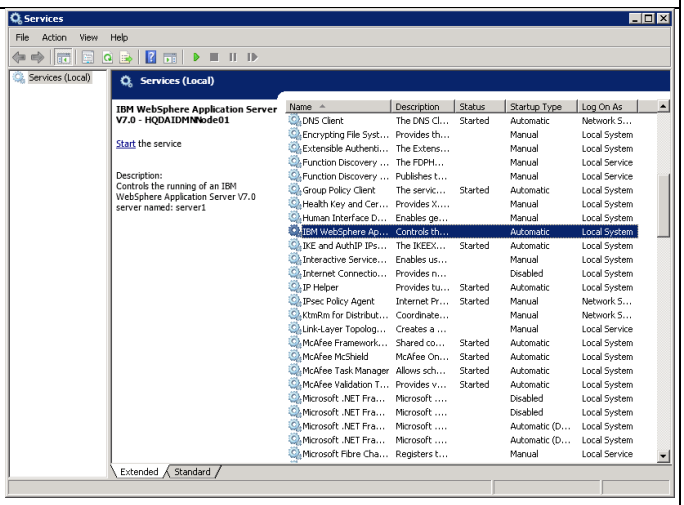
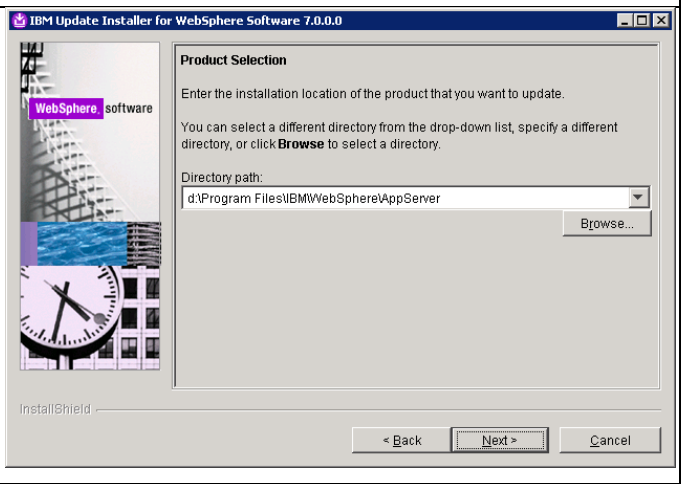
390

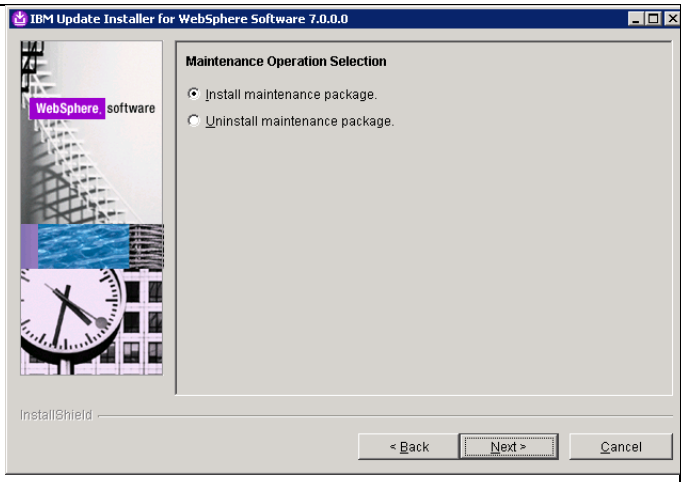
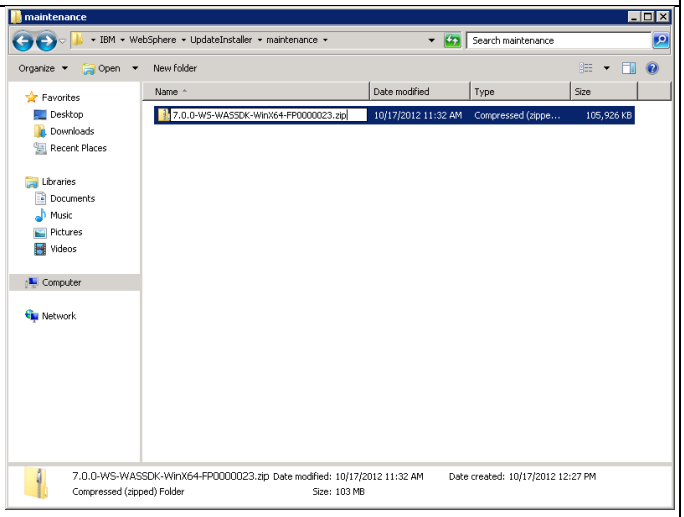
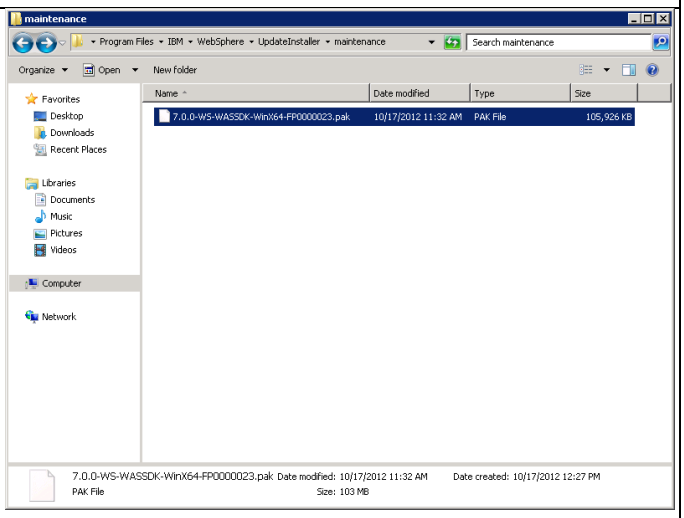
Haga clic en Siguiente	
Acepte el acuerdo de licencia	
Haga clic en Siguiente	

391

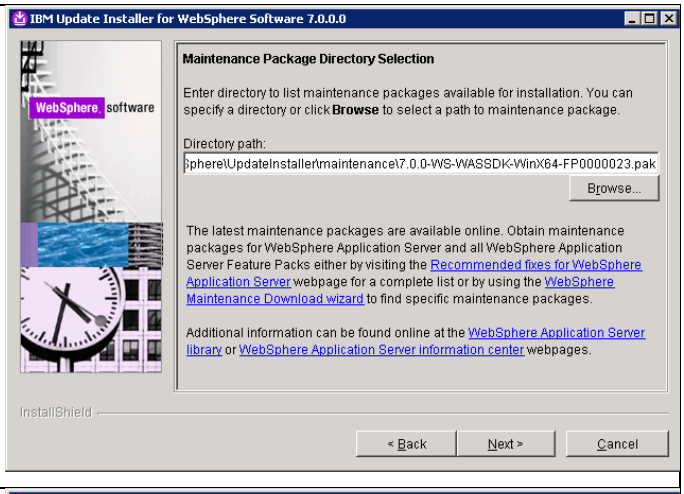
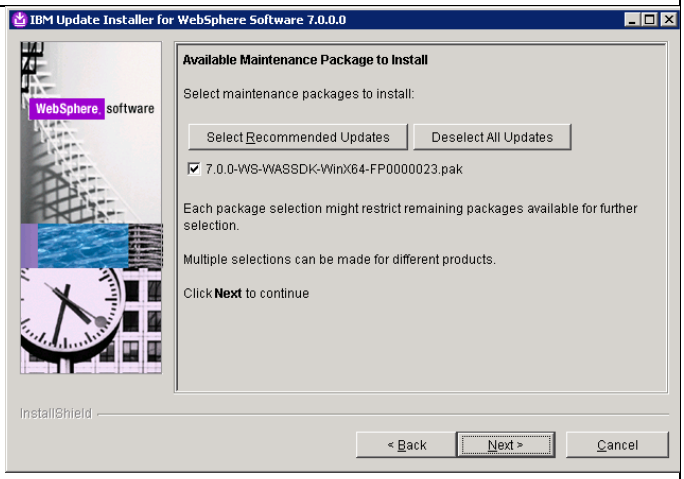
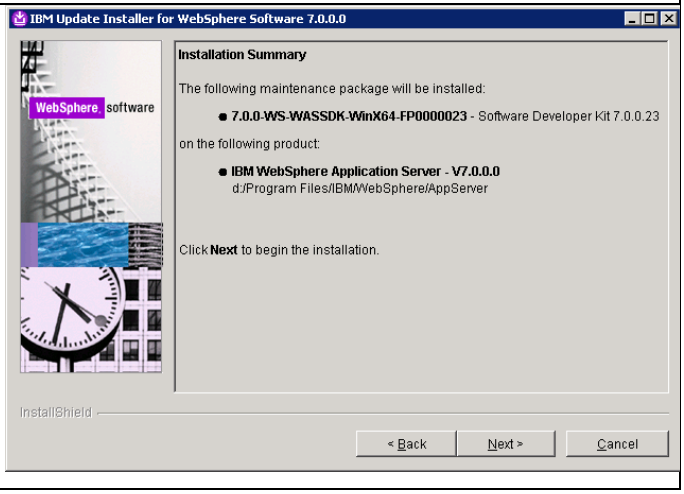
Especifique la ruta de instalación	
Revise el resumen de la instalación	
Después de la instalación de lanzar la actualización	

392

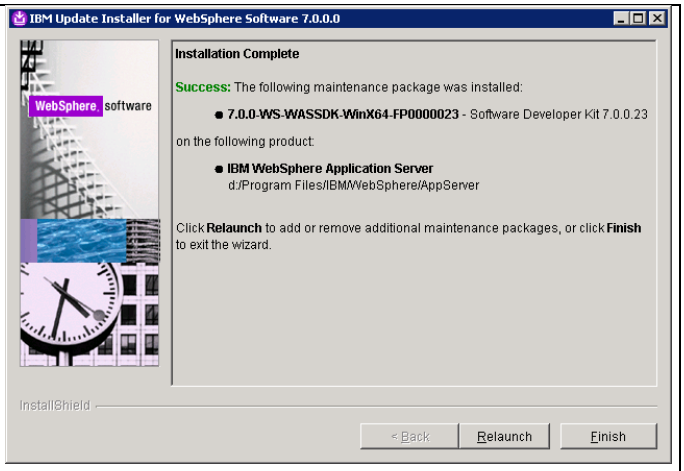
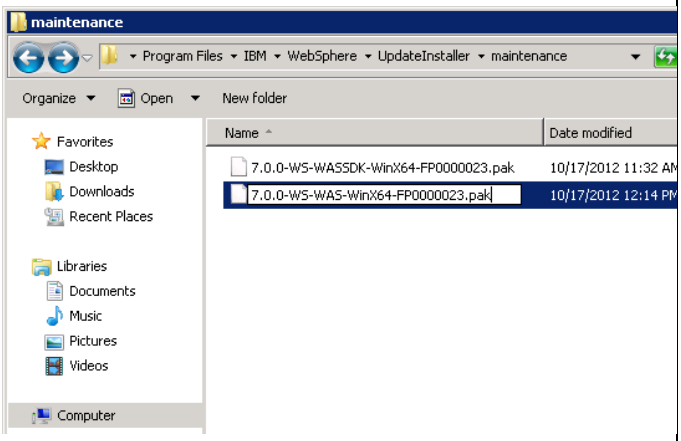
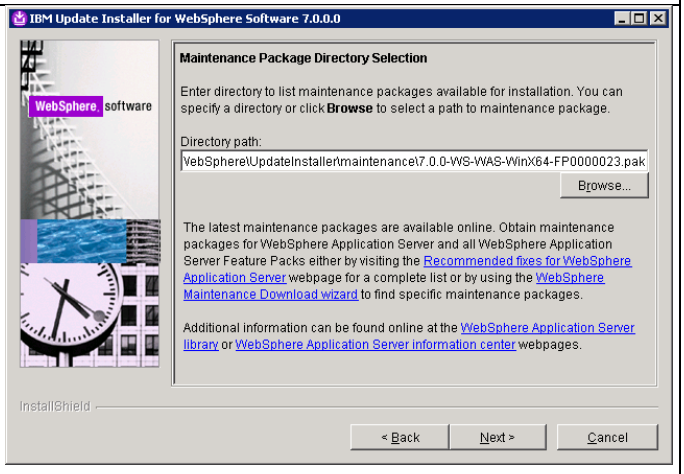
Haga clic en Siguiente	
Detenga el servicio de WebSphere	
Compruebe la ubicación del servidor de aplicaciones	

Seleccione el paquete de mantenimiento de instalación	
Cambiar la extensión SDK postal era un .pak y copiarlo a la carpeta de mantenimiento instalador de actualizacione	
Archivo cambiado a .pak pantalla	

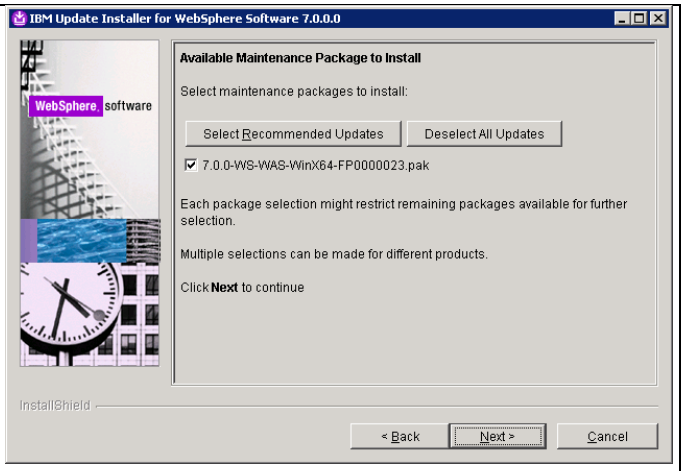
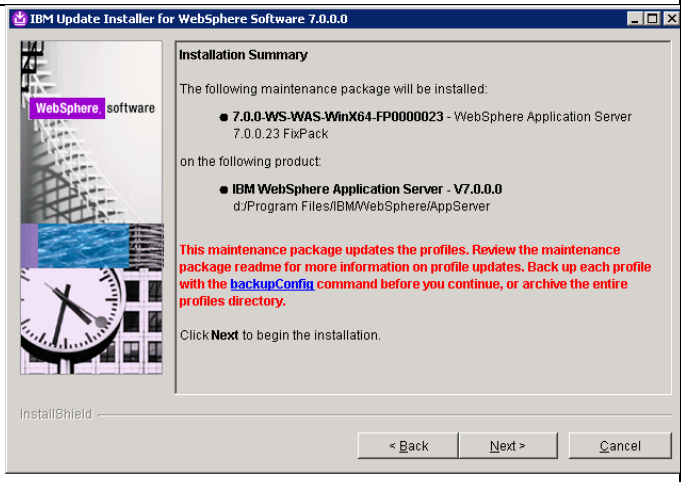
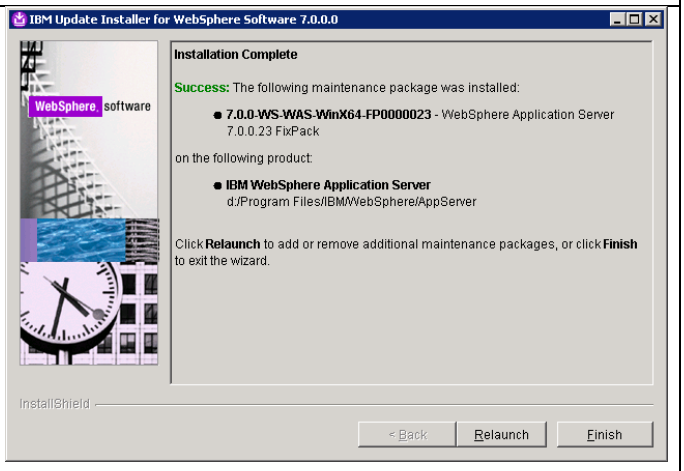
394

Manualmente entrar en el camino de la WASSDK en la ruta del directorio D: \ Archivos de programa \ IBM \ WebSphere \ UpdateInstaller \ mantenimiento \ 7.0.0 -WS - WASSDK - Winx64 - FP0000023.pak	
Compruebe que la casilla de verificación está seleccionada y haga clic en siguiente	
Verifique el resumen de la instalación y haga clic en siguiente	

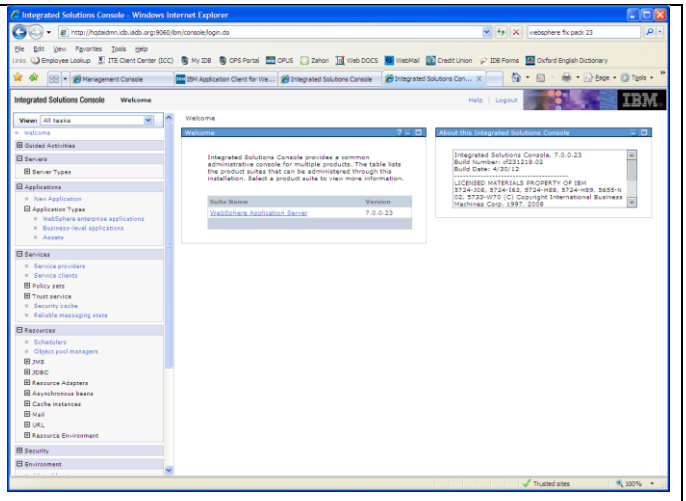
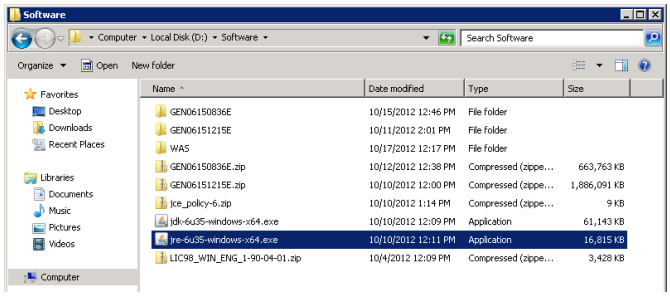
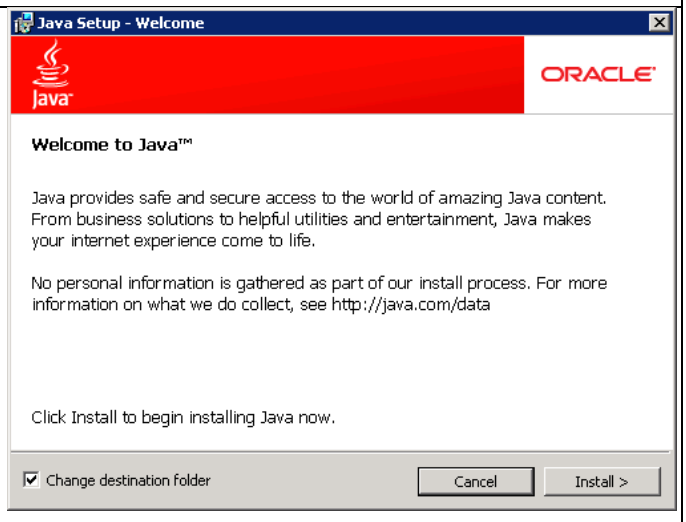
395

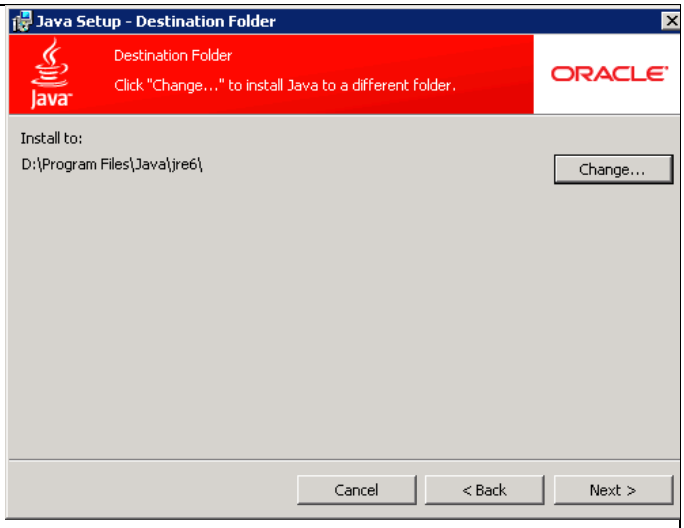
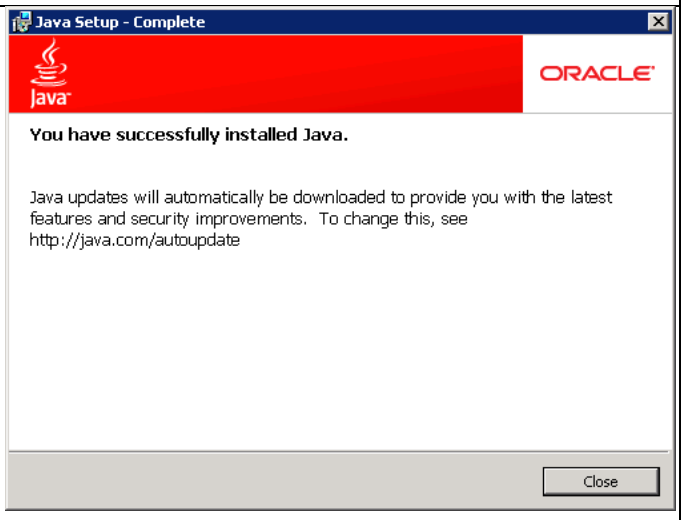
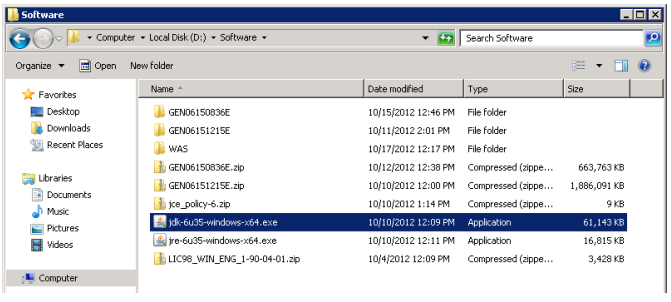
Haga clic relanzamiento	
Cambie la extensión zip a Pak y copiar a la carpeta de mantenimiento	
Navegar de vuelta a la selección directorio del paquete de mantenimiento y seleccione el WAS fixpack . Introduzca la ubicación manualmente	

396

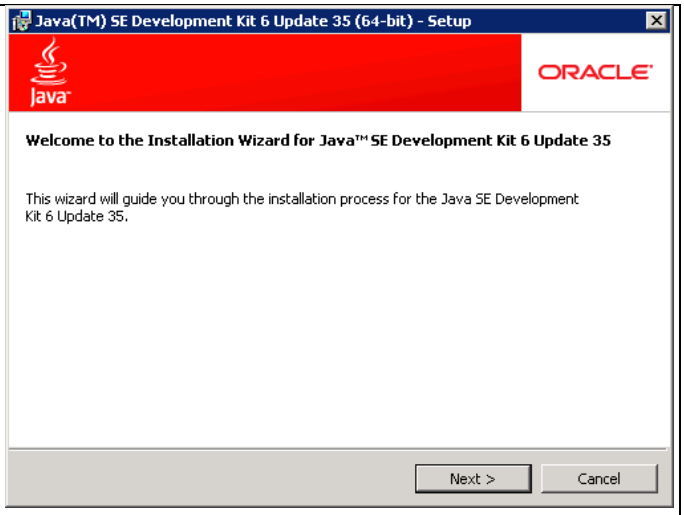
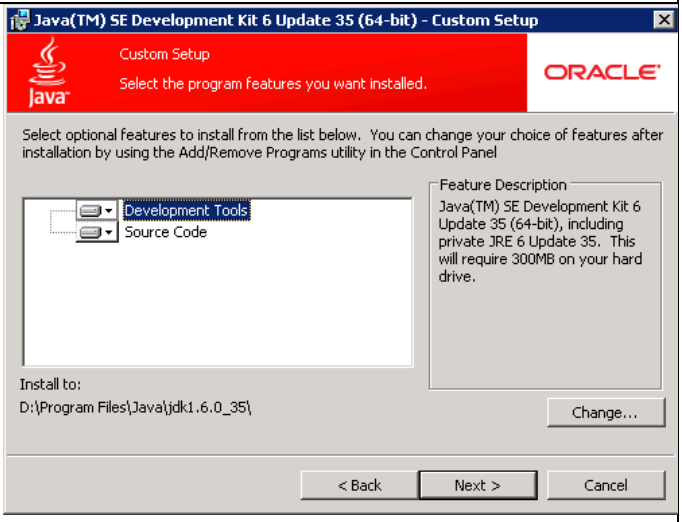
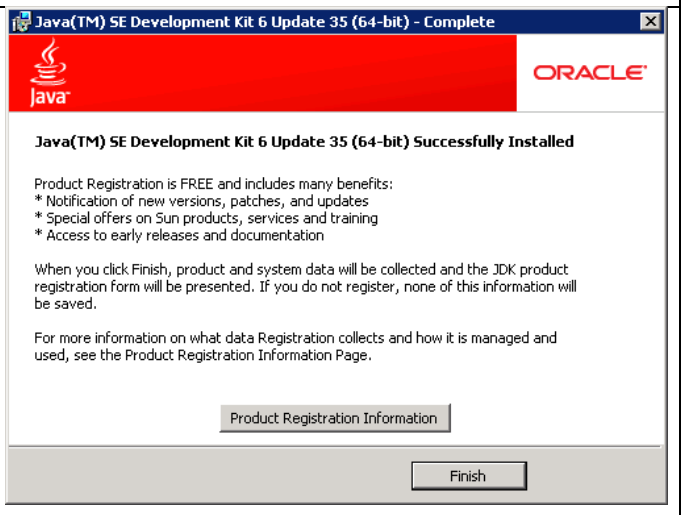
Asegúrese de que está seleccionada la casilla de verificación fixpack	
Verifique el resumen de la instalación	
Haga clic en Finalizar en la pantalla completa la instalación	

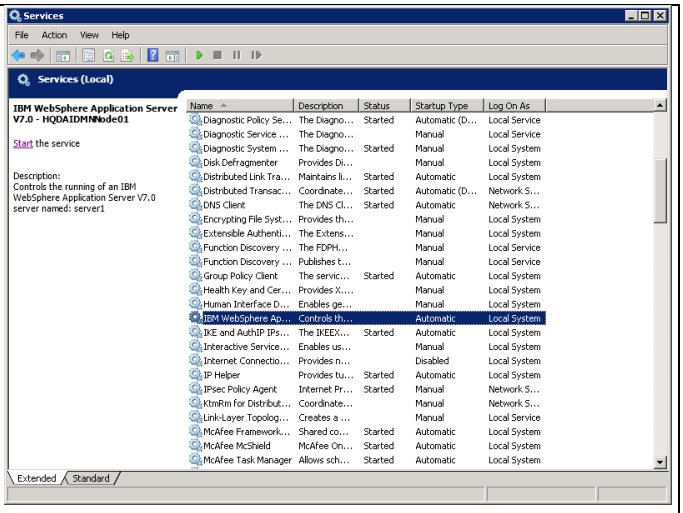
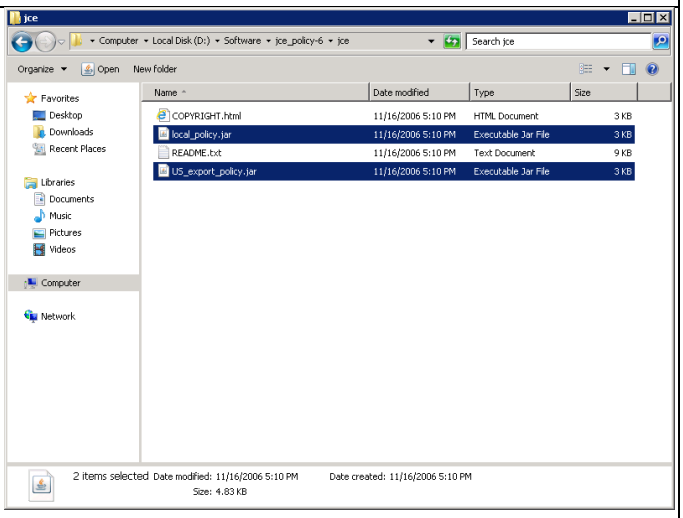
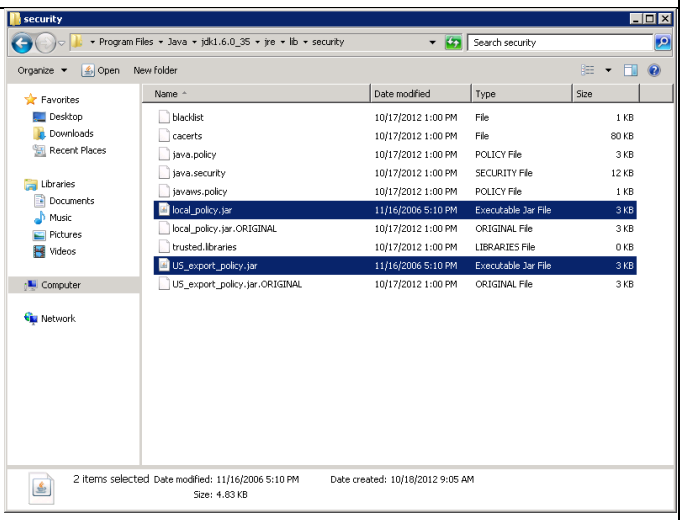
397

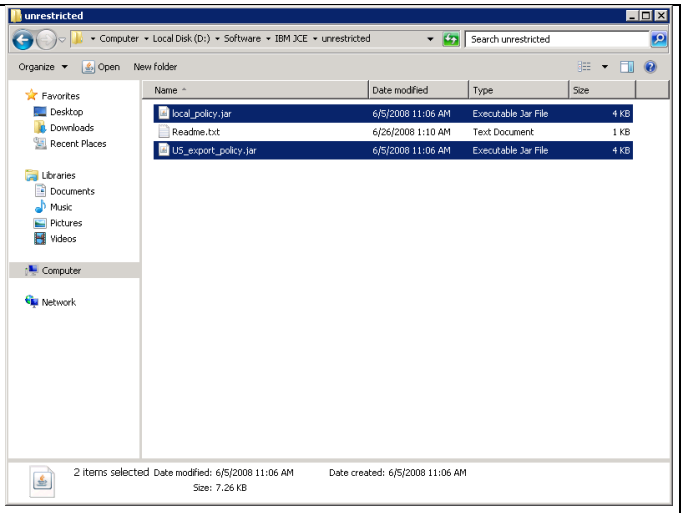
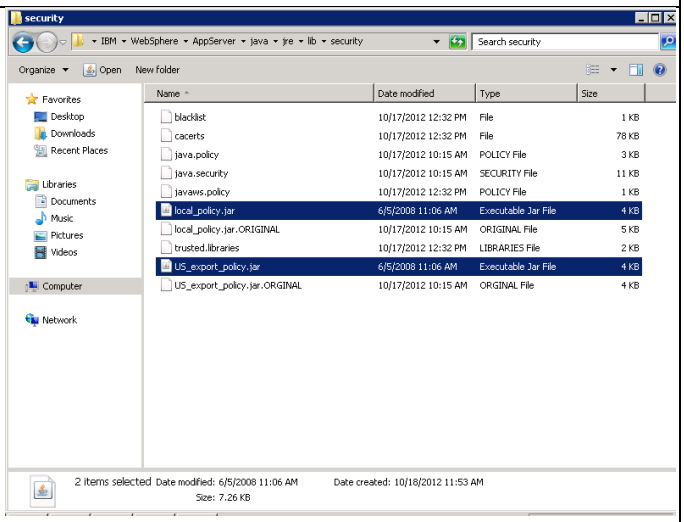
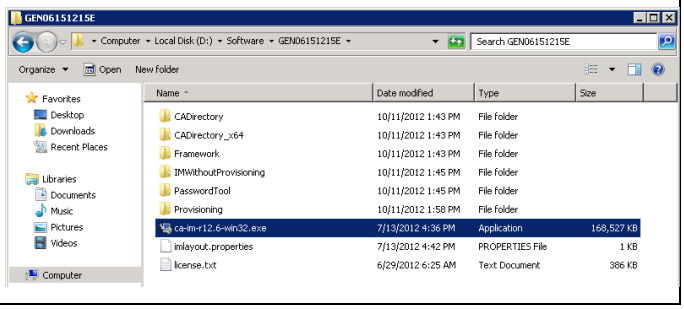
Compruebe que estaba en la versión 23	
Haga clic en el medio de instalación de JRE	
Seleccione la casilla de verificación carpeta de destino	

Cambie a la unidad D y haga clic en Siguiente	
Haga clic en Cerrar después de la instalación	
Instale el JDK haciendo clic en el medio de instalación	

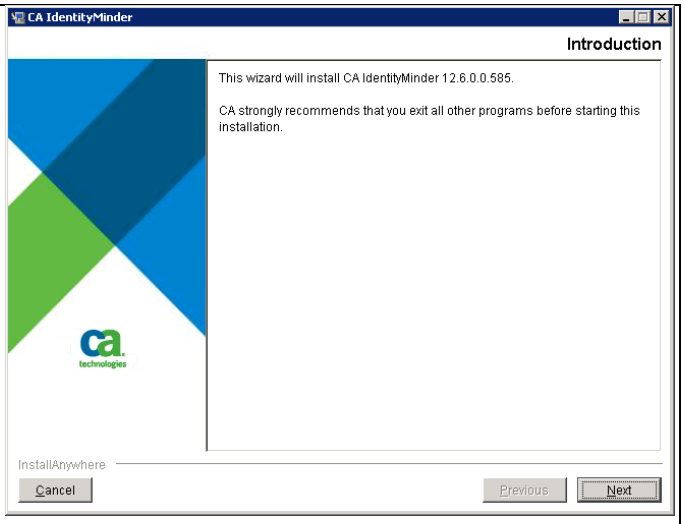
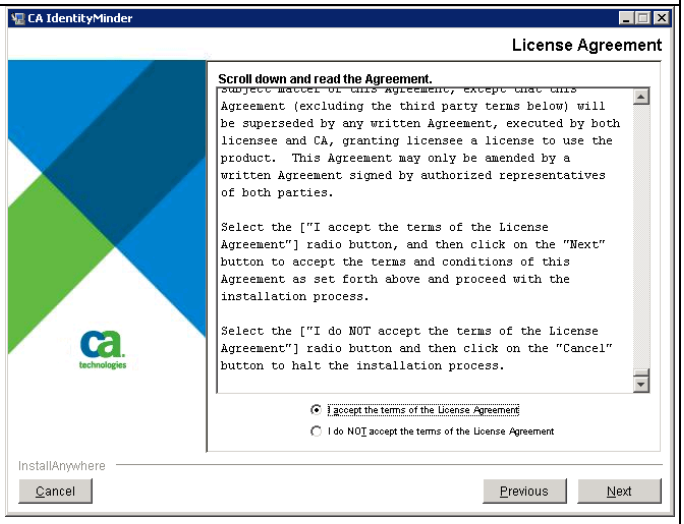
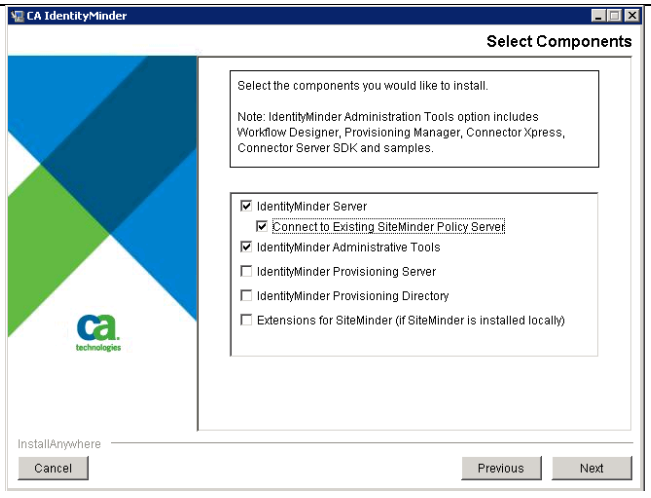
399

Haga clic en Siguiente	
Cambie a la unidad D	
Haga clic en Finalizar	

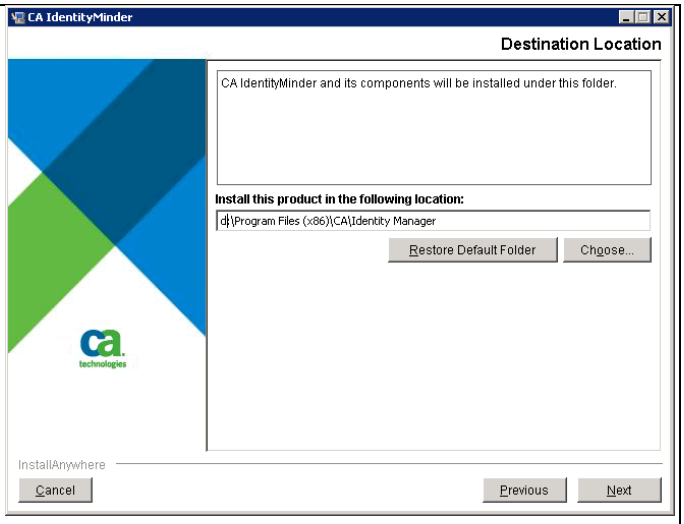
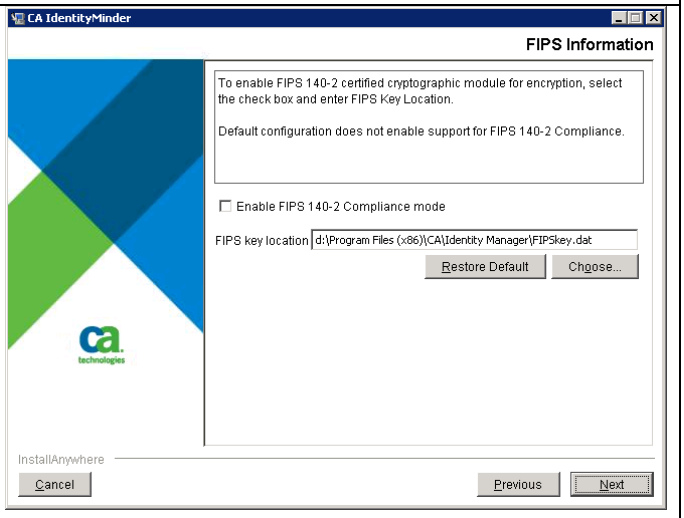
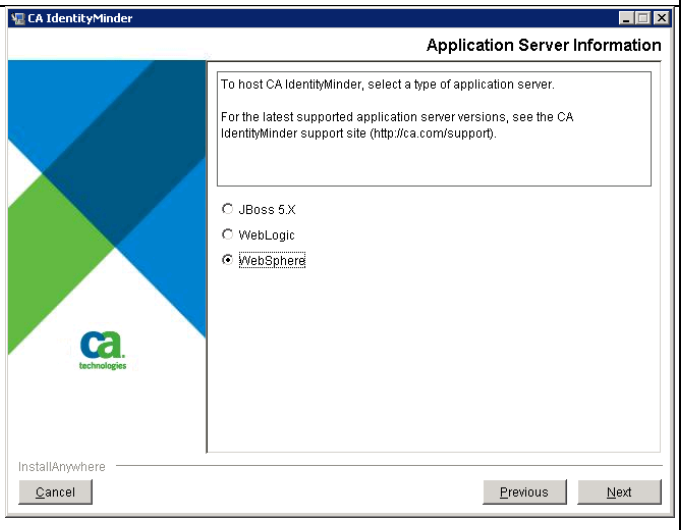
Detenga WebSphere	
Copiar sobre la JCE de la carpeta de software	
Pegue la JCE en la carpeta de seguridad jdk (renombrar archivos originales)	

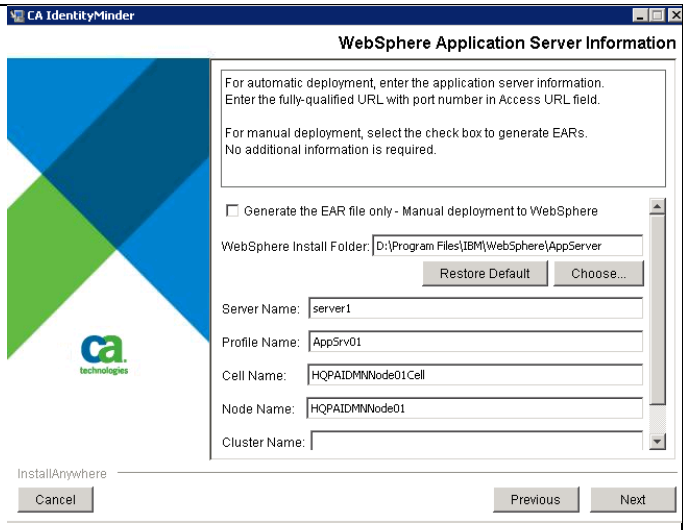
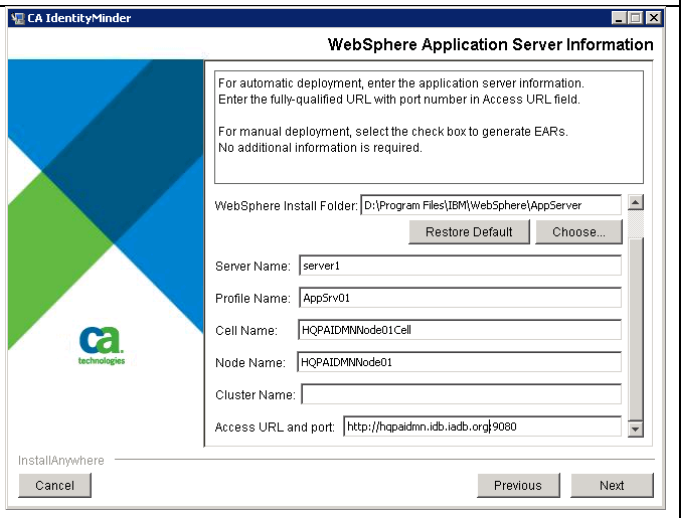
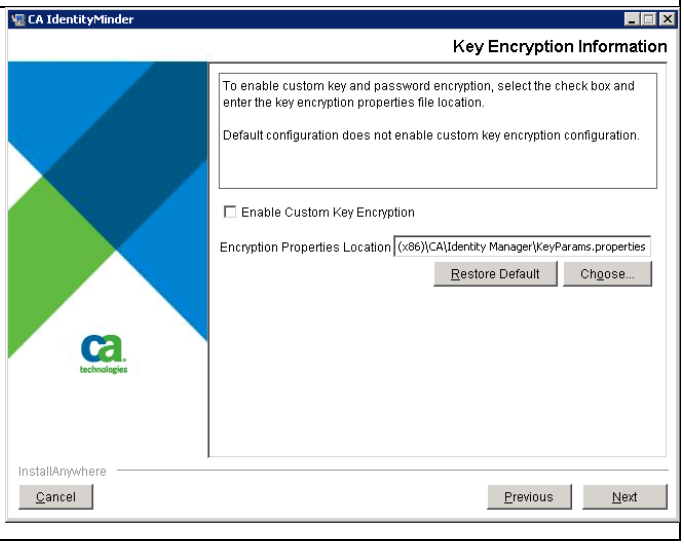
Copie sobre IBM JCE de la carpeta de software	
Pegue JCE en la trayectoria de IBM JRE (Renombrar el original)	
Haga clic en la ca- im - r12.6 - win32.exe desde el medio de instalación	

402

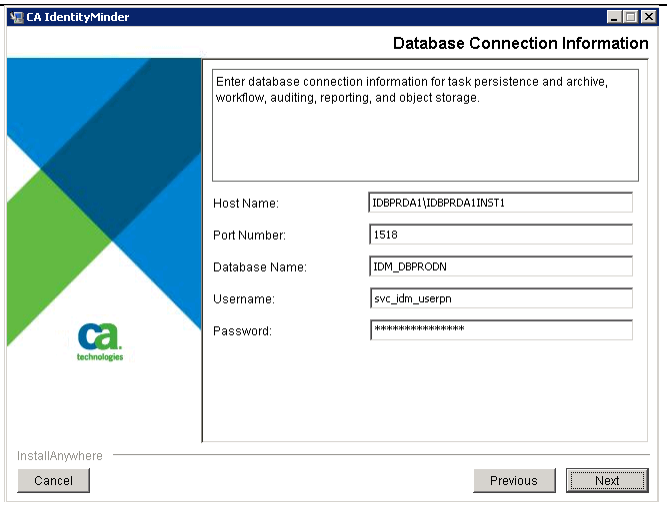
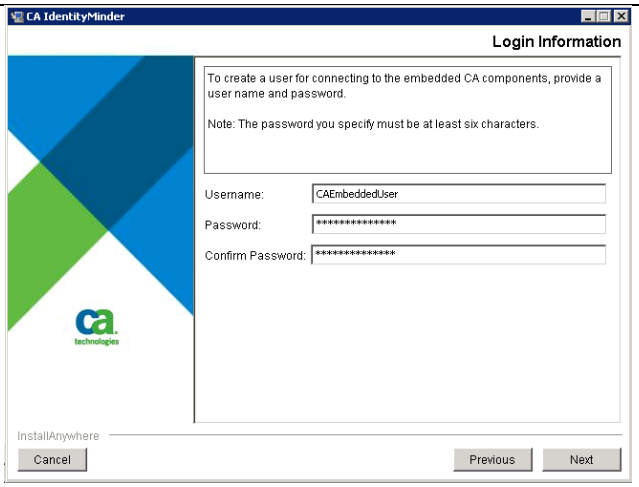
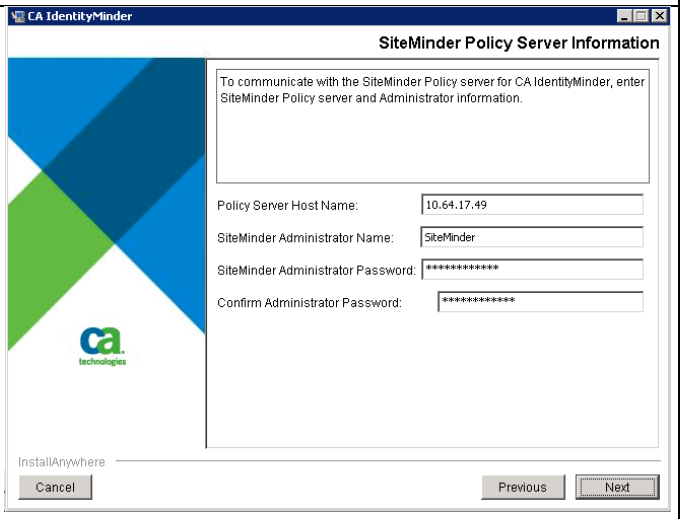
Haga clic en Siguiente	
Acepte los acuerdos de licencia	
Seleccione las casillas de verificación que se muestran 3	

403

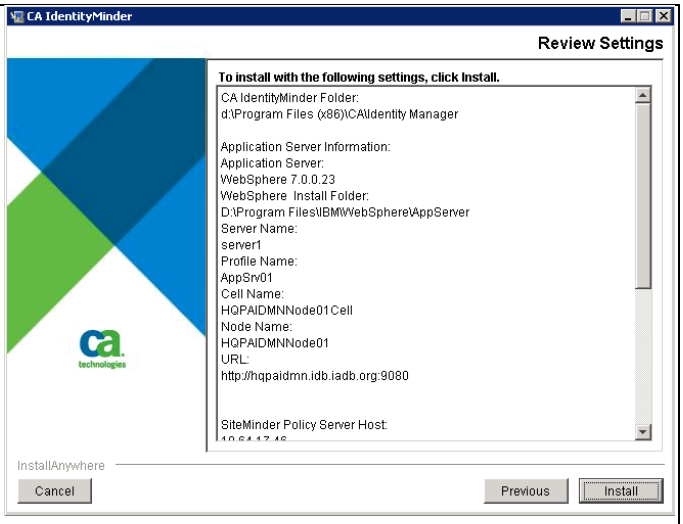
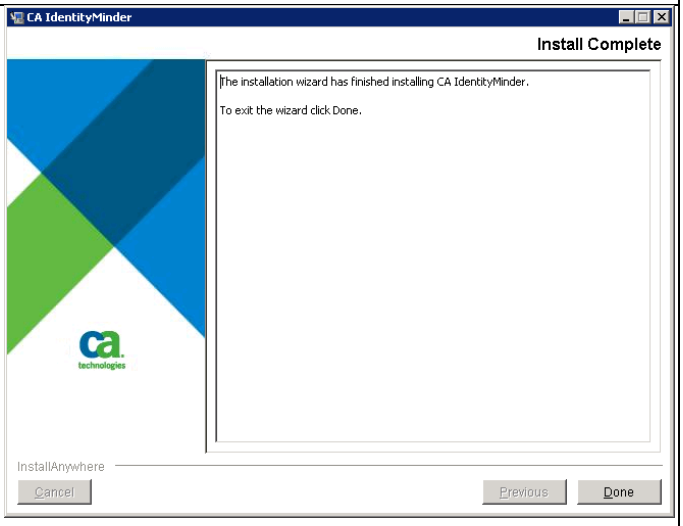
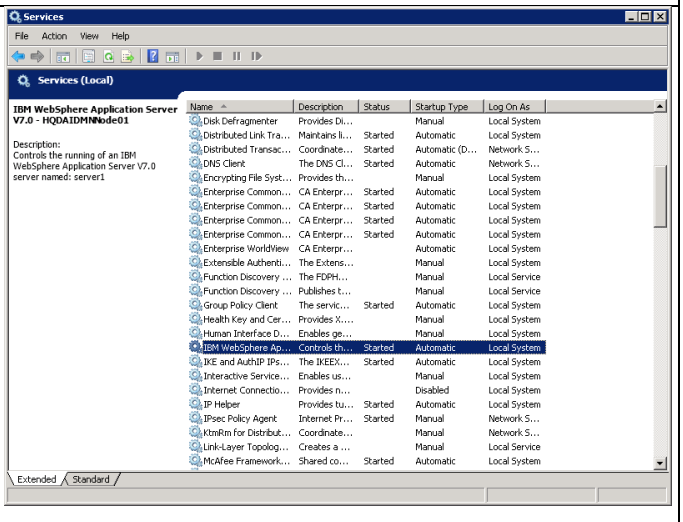
Cambiar la ruta de instalación en la unidad D	
Desmarque habilitar FIPS	
Seleccione WebSphere	

Ingrese la información ha demostrado	
Introduzca el puerto de acceso url ha demostrado	
Cifrado Desmarque clave personalizada incapaces	

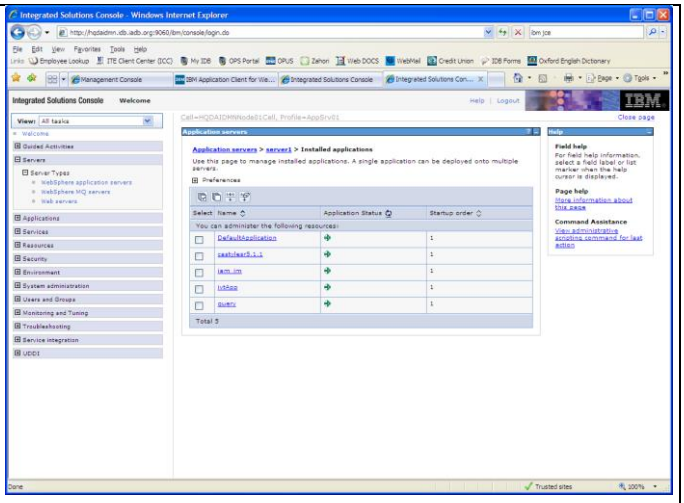
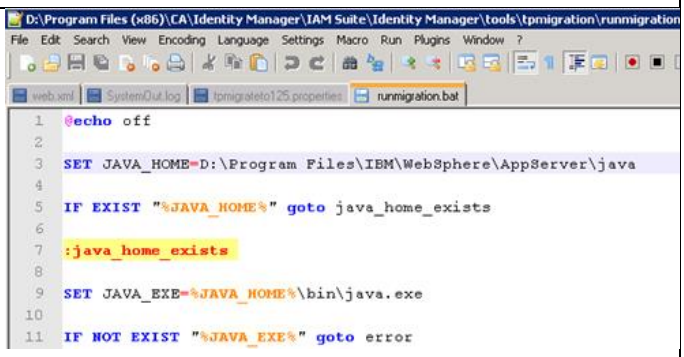
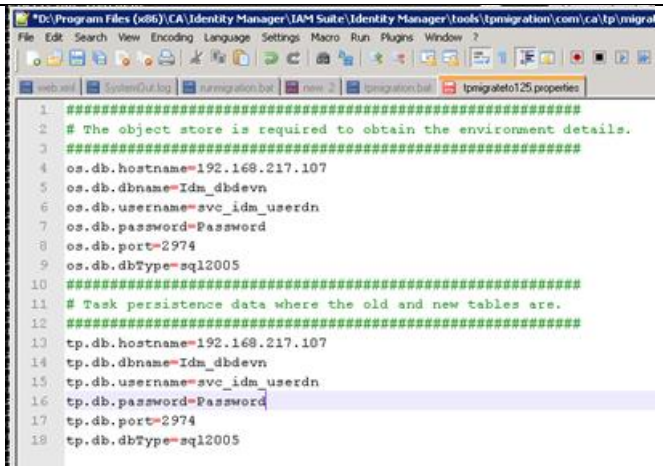
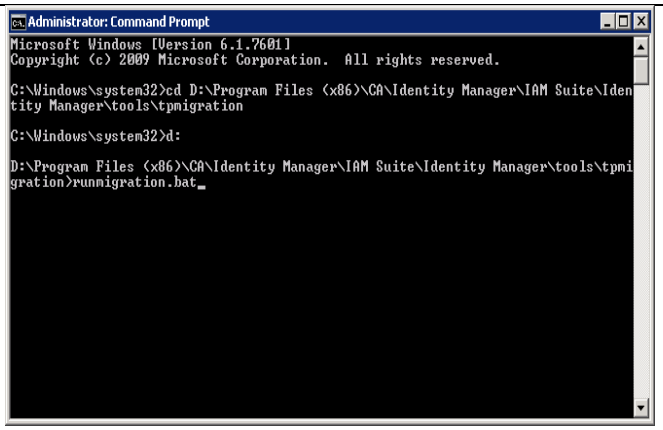
405

Puede ser el uso de un puerto diferente en PROD	
Introduzca el nombre de usuario y la contraseña para el usuario incrustado	
Introduzca la información de la cuenta de SiteMinder que se utilizará para hacer conexiones	

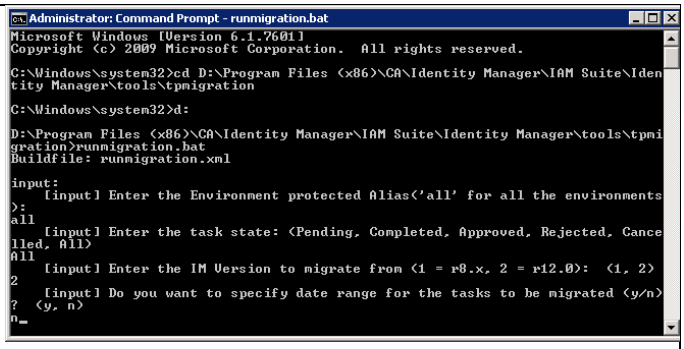
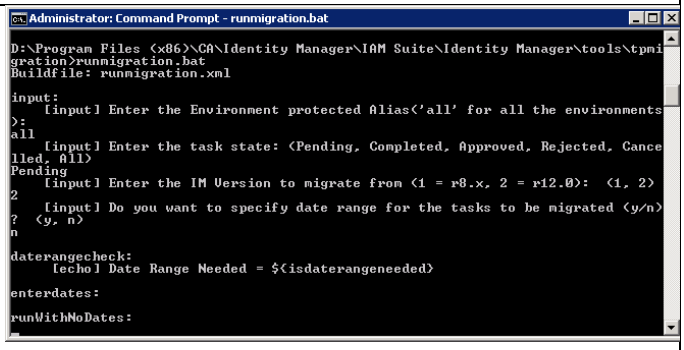
406

Verifique el resumen de la instalación	
Haga clic en Hecho	
	

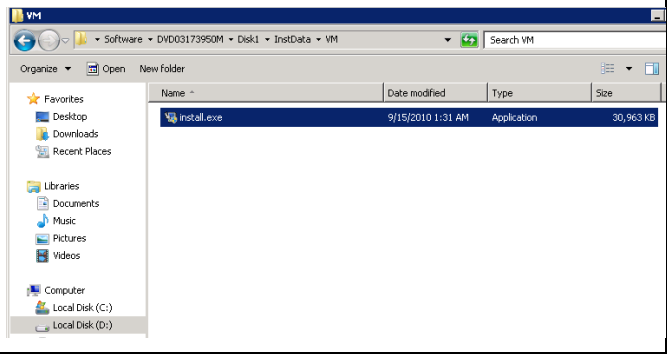
407

	
Compruebe que JAVA_HOME está establecido. (Ya sea en las variables de entorno o el archivo por lotes runmigration) D: \ Archivos de programa (x86) \ CA \ Identity Manager \ IAM Suite de \ Identity Manager \ tools \ tpmigration \ runmigration.bat	
Se presentar los tpmigration125.properties con la información adecuada , como se muestra .	
En una pantalla de símbolo del sistema vaya a la ubicación del archivo runmigraion.bat	

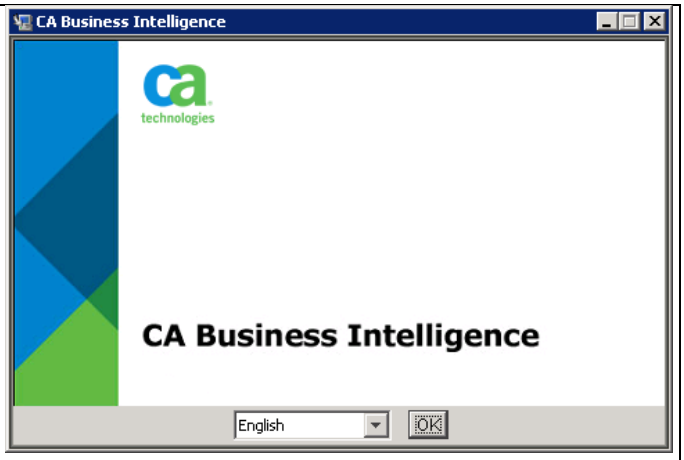
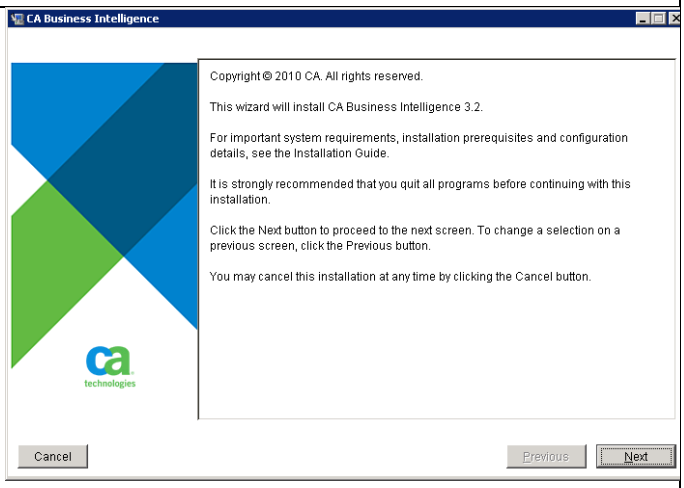
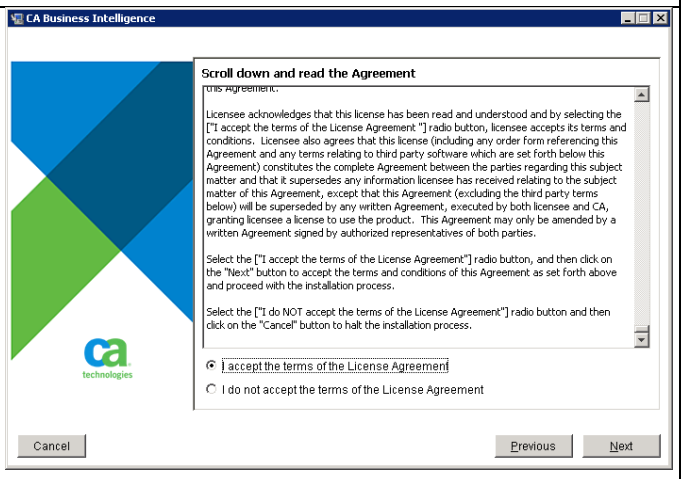
408

En las instrucciones introduzca los siguientes valores : todas Todas 2 n	
Ejecute runmigration.bat presentar una segunda vez e introduzca los valores siguientes en el símbolo del sistema : todas A la espera de 2 n	

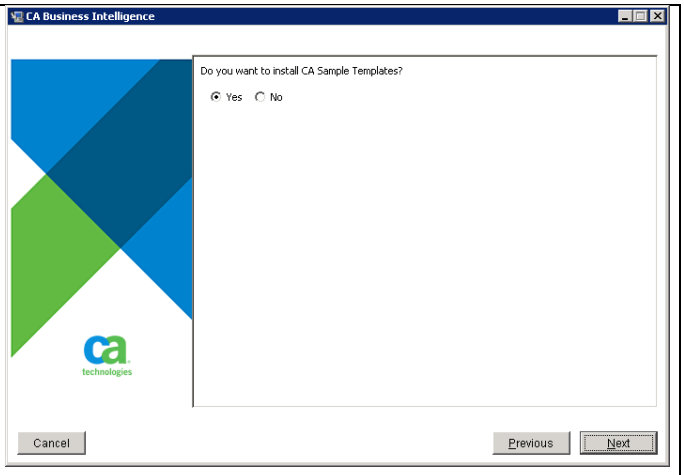
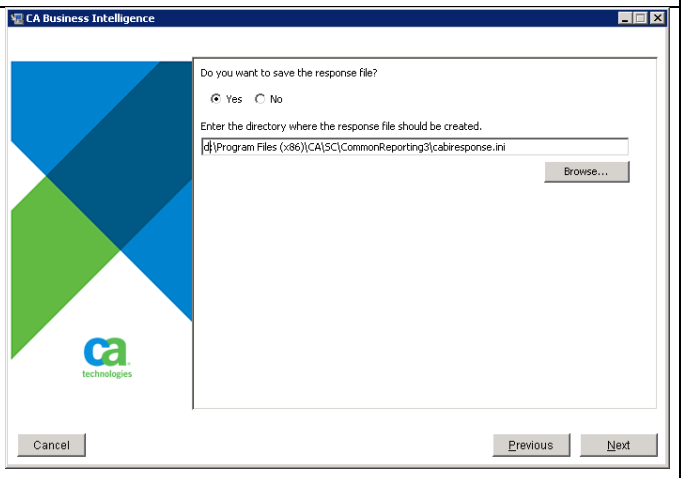
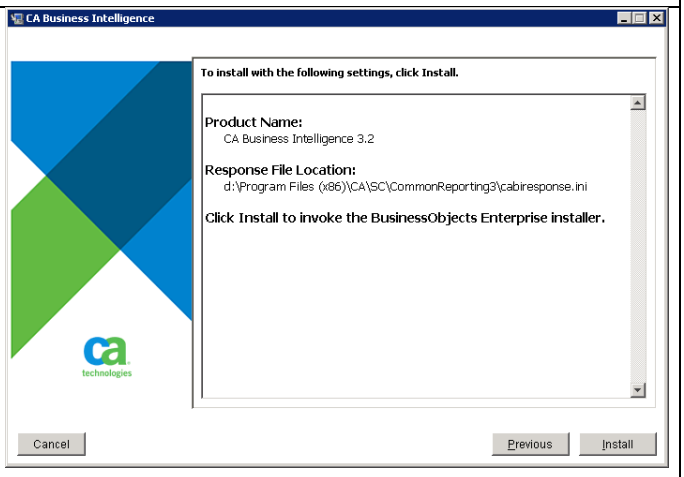
2.1.12 Instalar informe CA Identity Manager

2.1.13 Instalar informe CA Identity Manager	
Navegue hasta el directorio que se muestra	

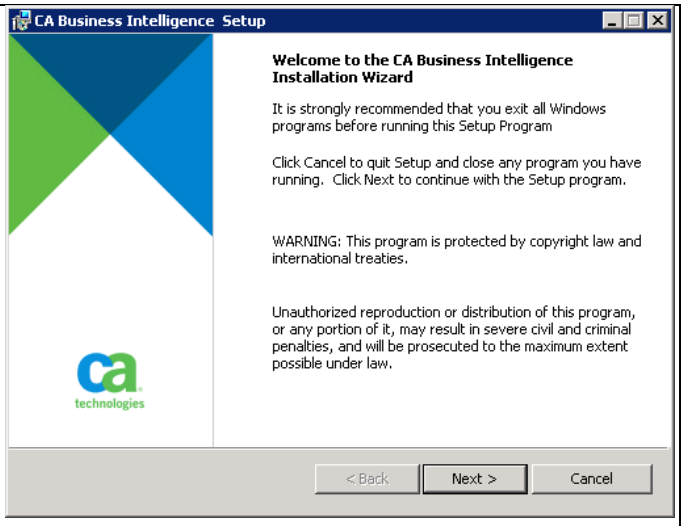
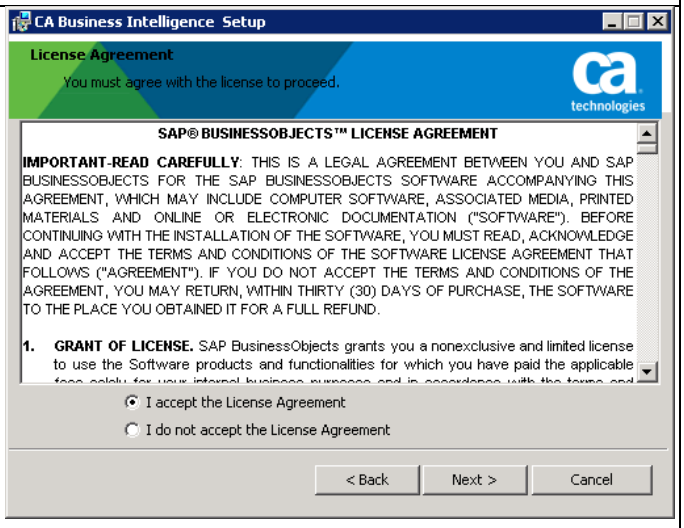
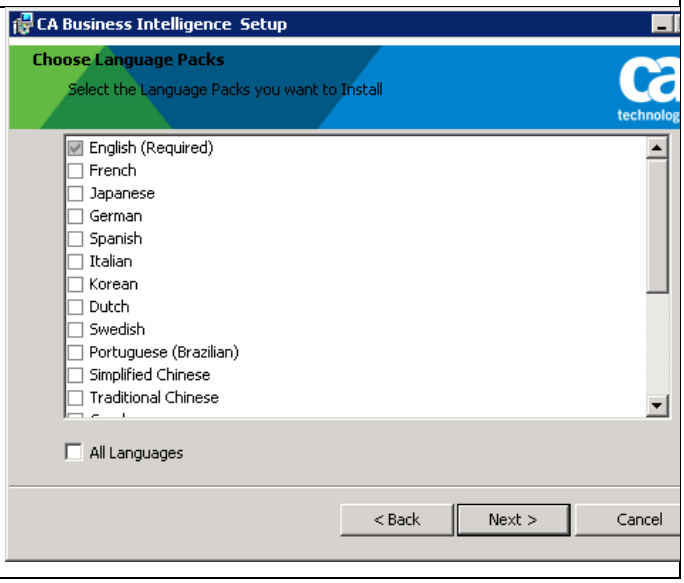
409

Haga clic en Aceptar	
Haga clic en Siguiente	
Aceptar los términos de licencia	

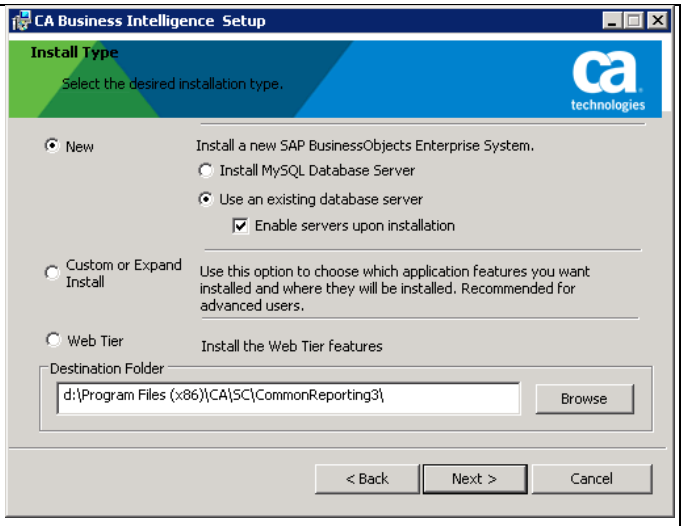
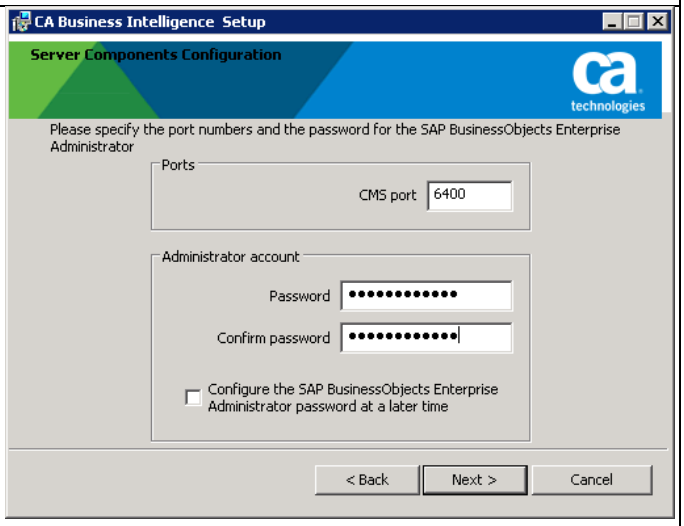
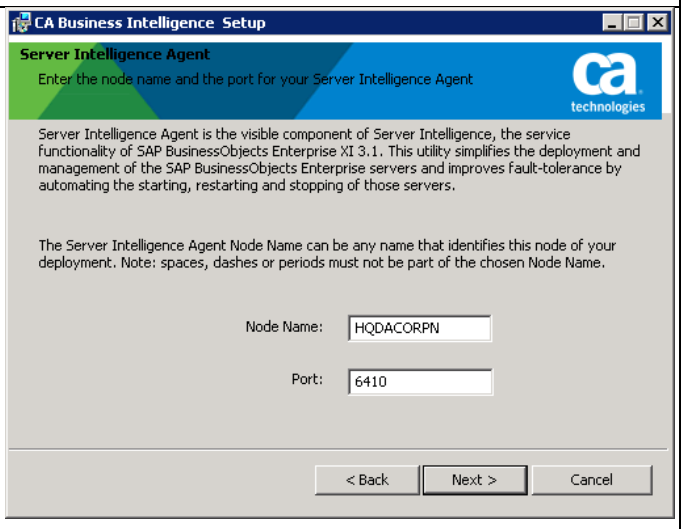
410

Haga clic en Sí para instalar las plantillas de ejemplo	
Cambiar la ruta de instalación para D	
resumen de la valoración	

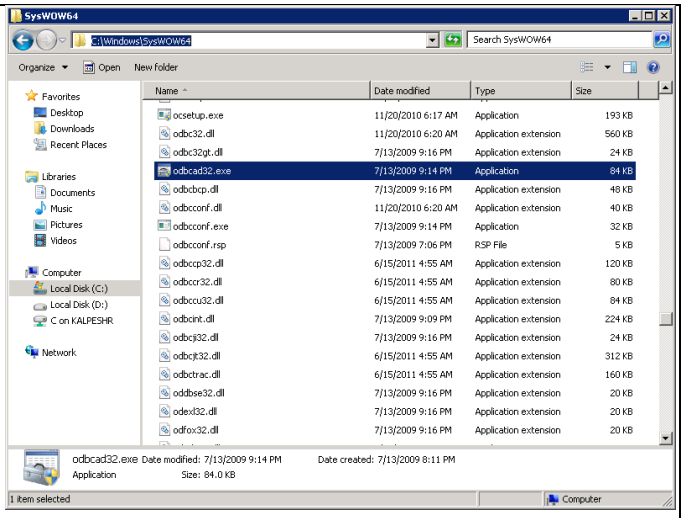
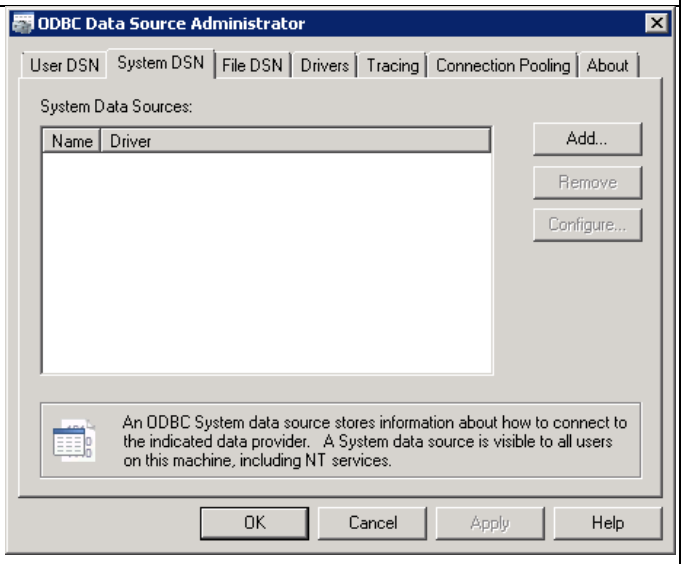
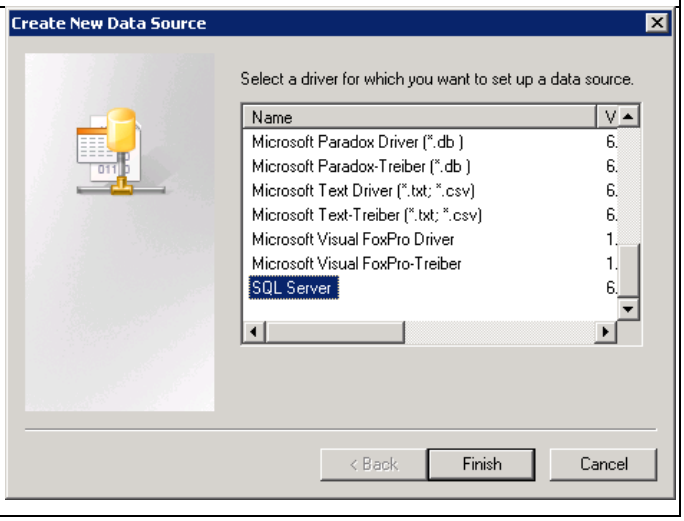
411

Haga clic en Siguiente	
Acepte los acuerdos de licencia	
Seleccione los idiomas correspondientes	

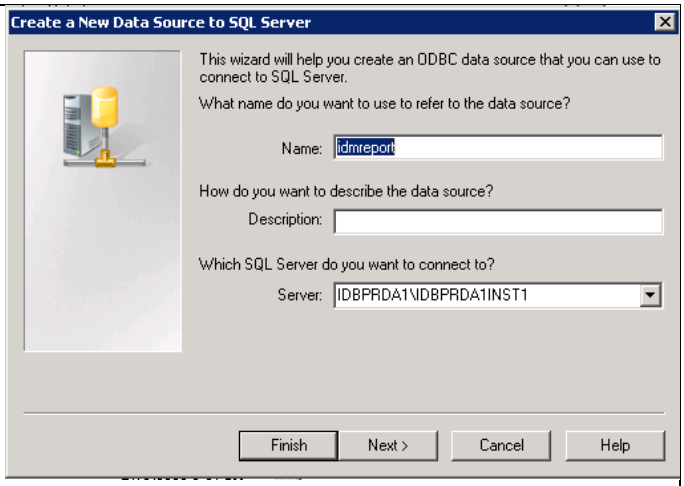
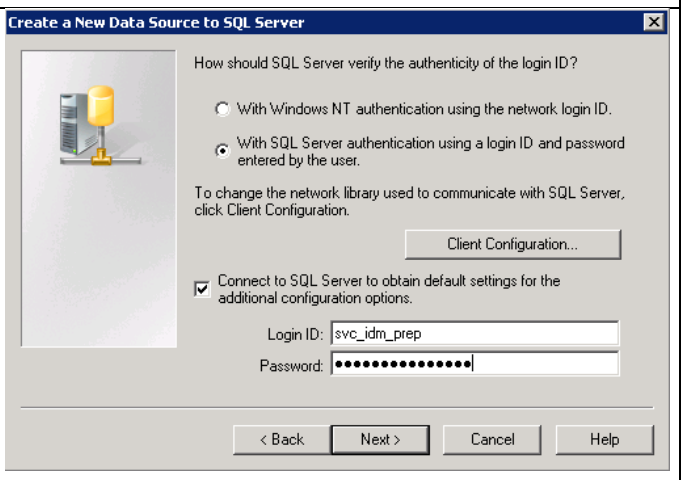
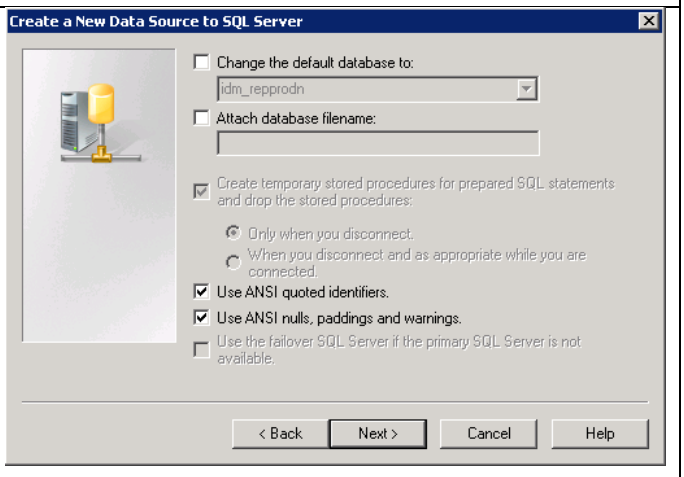
412

Ingrese la información mostrada en la pantalla	
Establezca la contraseña de la cuenta de administrador	
Compruebe la pantalla y haga clic en Siguiente	

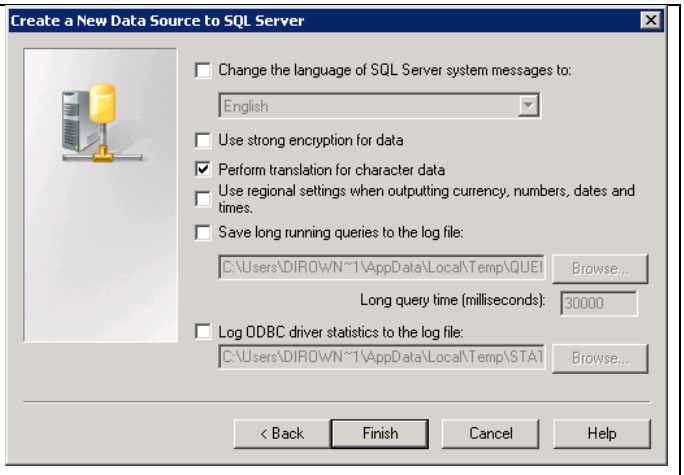
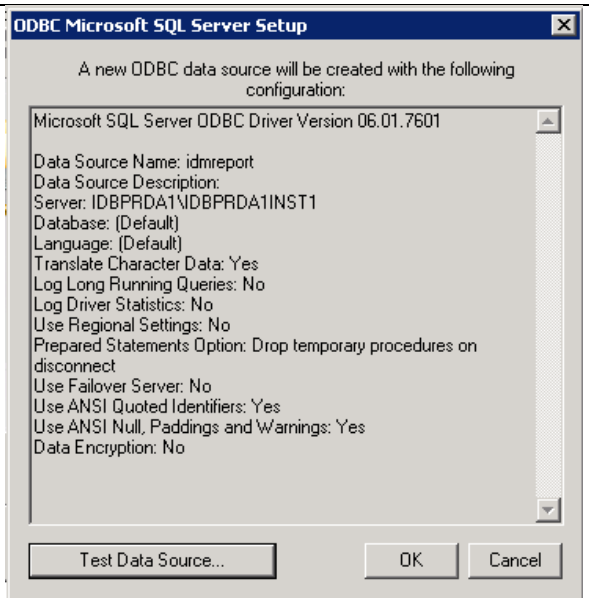
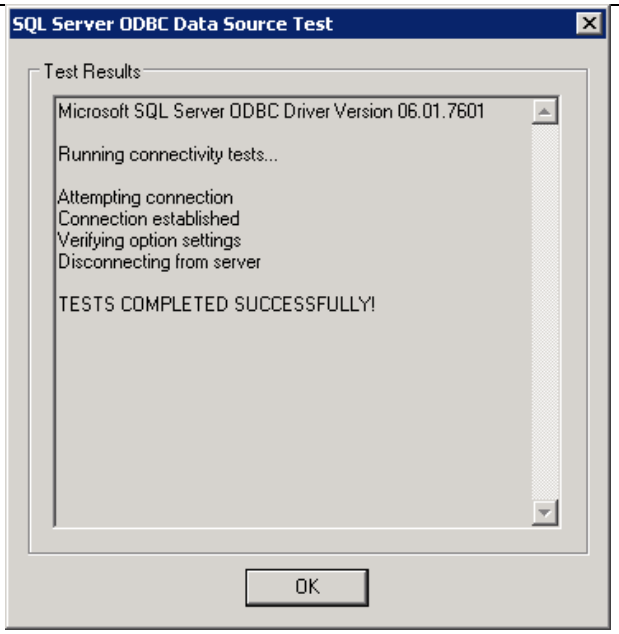
413

Vaya a C: \ Windows \ SysWOW64	
Haga clic en DSN de sistema	
Seleccione SQL Server y haga clic en Finalizar	

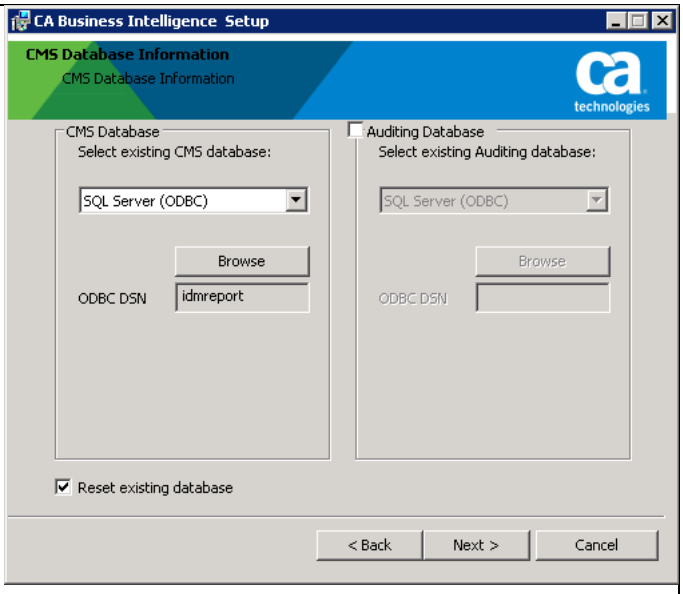
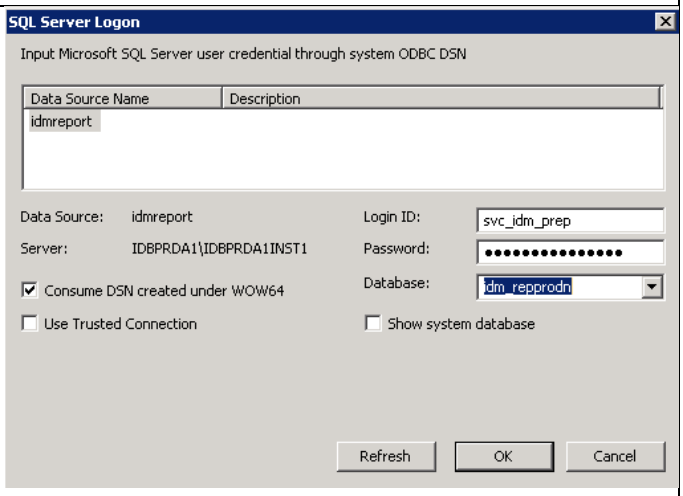
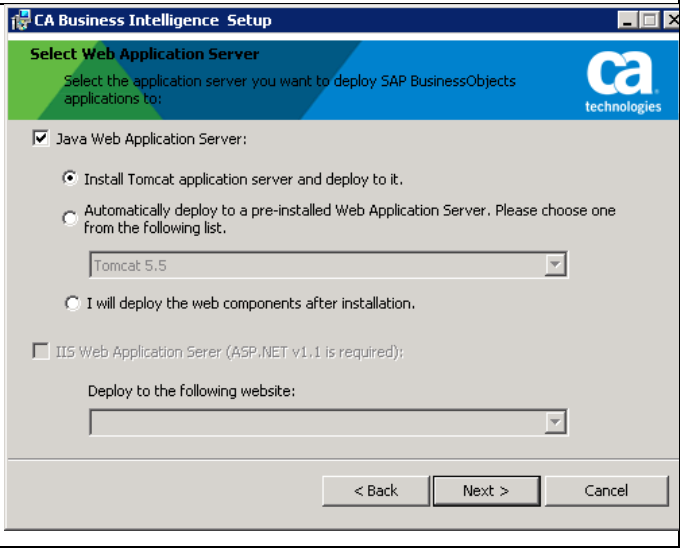
414

Ingrese la información mostrada	
Introduzca las credenciales de DB	
Verifique la casilla de verificación es como se muestra	

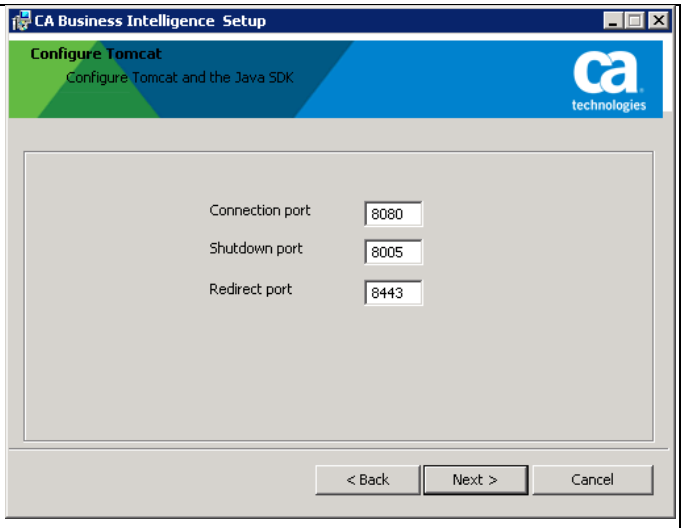
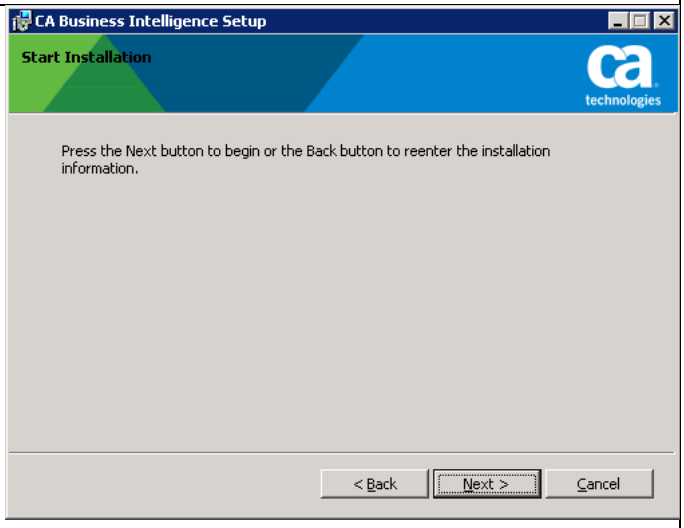
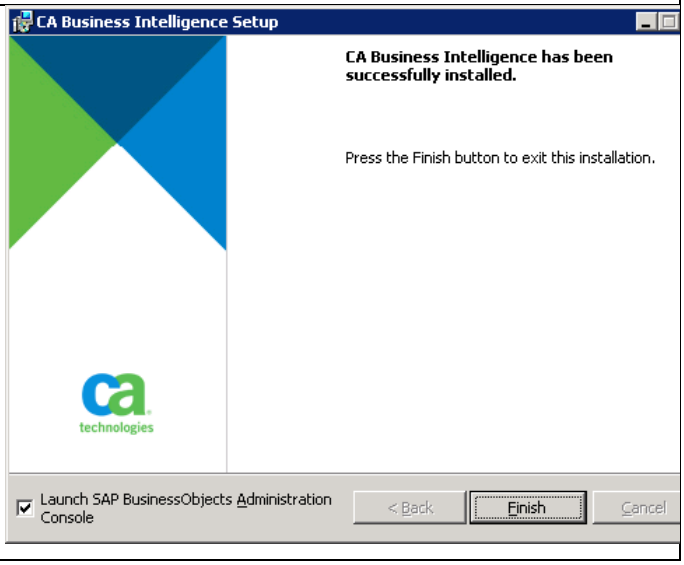
415

Haga clic en Finalizar	
Fuente de datos de prueba	
Haga clic en Aceptar	

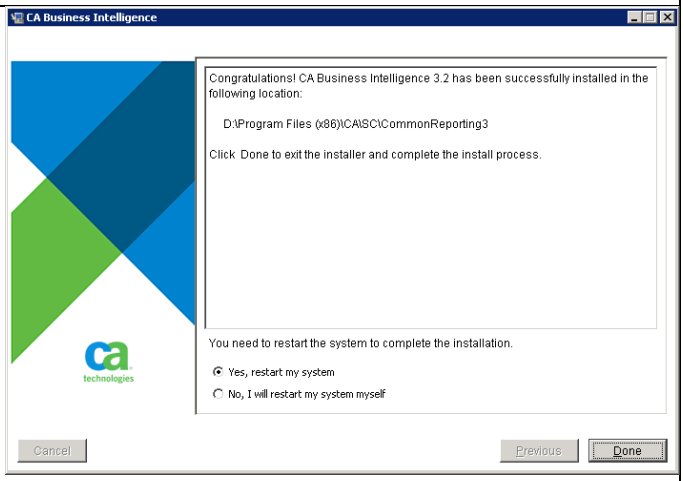
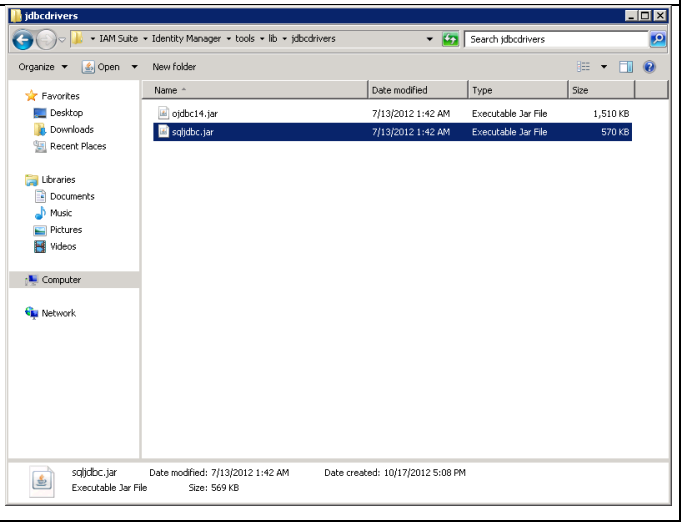
416

Ingrese la información como se muestra (Haga clic en Examinar para establecer idmreport)	
Verifique la pantalla seleccionada es como se muestra	
Seleccione Java servidor de aplicaciones Web e instalar Tomcat	

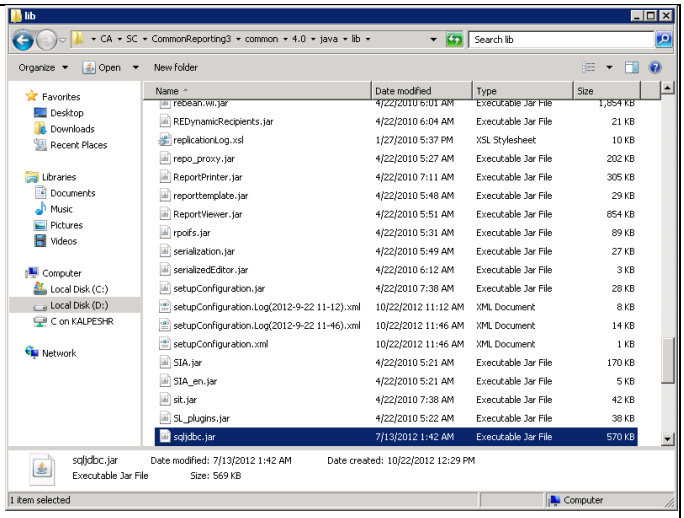
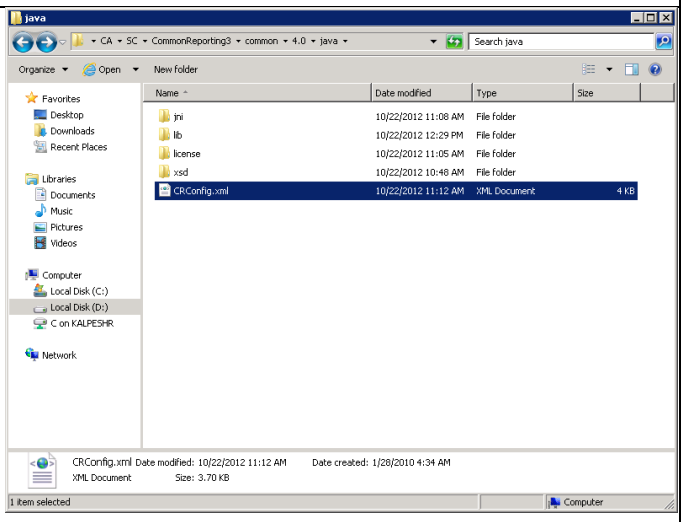
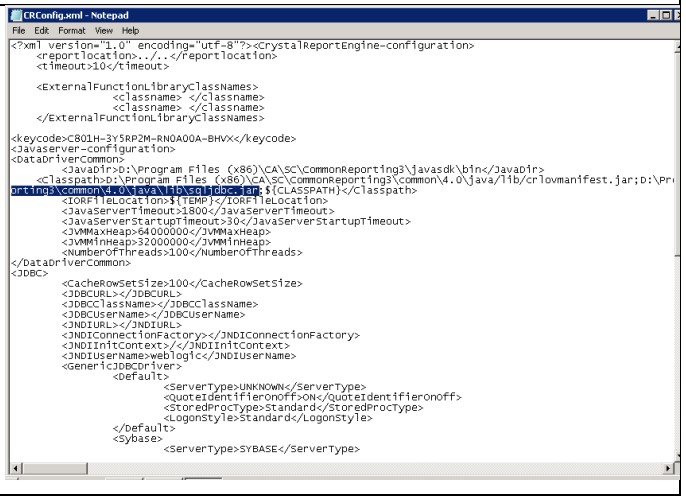
417

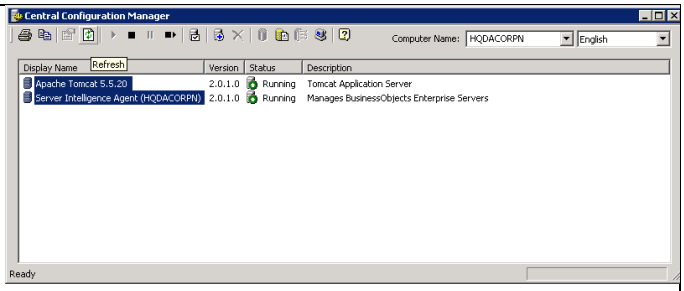
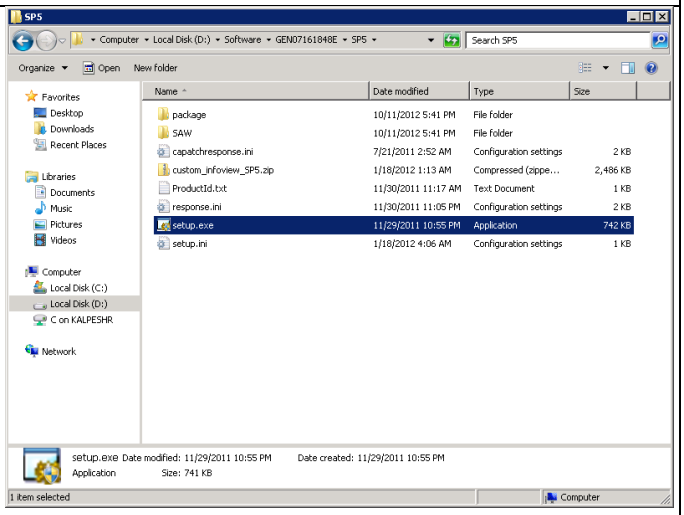
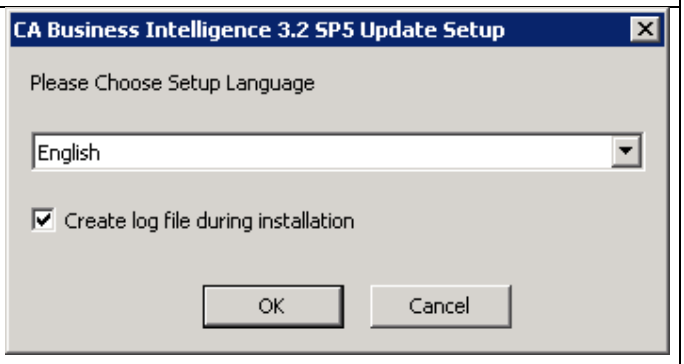
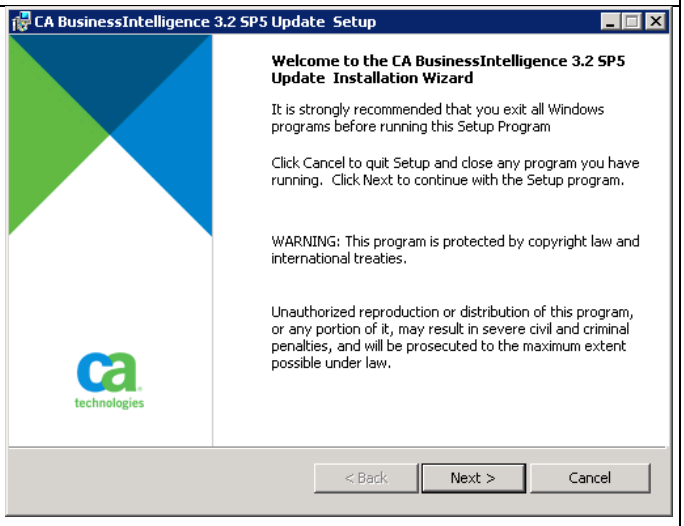
Deje los puertos predeterminados	
Haga clic en Finalizar	
Haga clic en Finalizar	

418

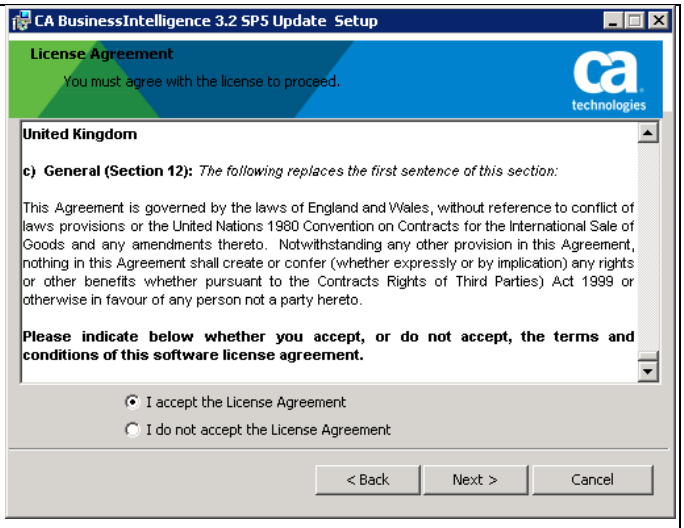
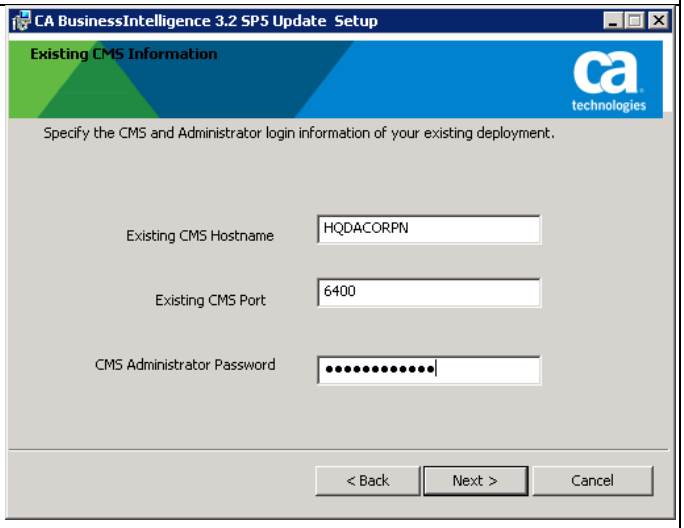
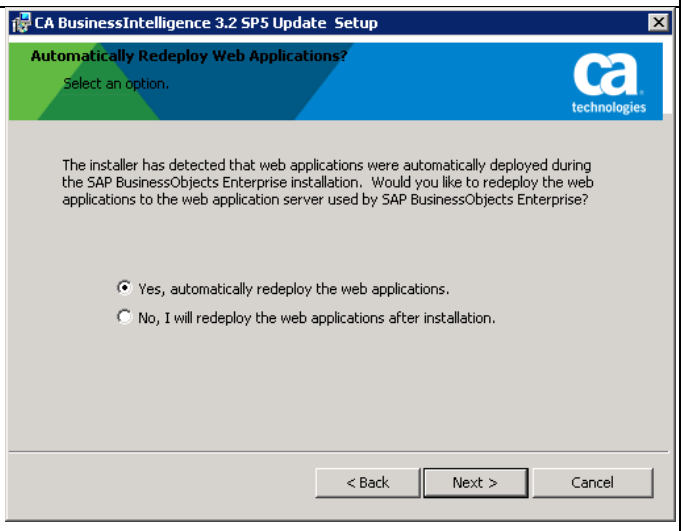
Deje que el proceso de	
Reinicie el servidor	
Desde el servidor de Identity Manager obtener el archivo sqljdbc.jar archivo de: D: \ Archivos de programa (x86) \ CA \ Identity Manager \ IAM Suite de \ Identity Manager \ tools \ lib \ jdbcdrivers	

419

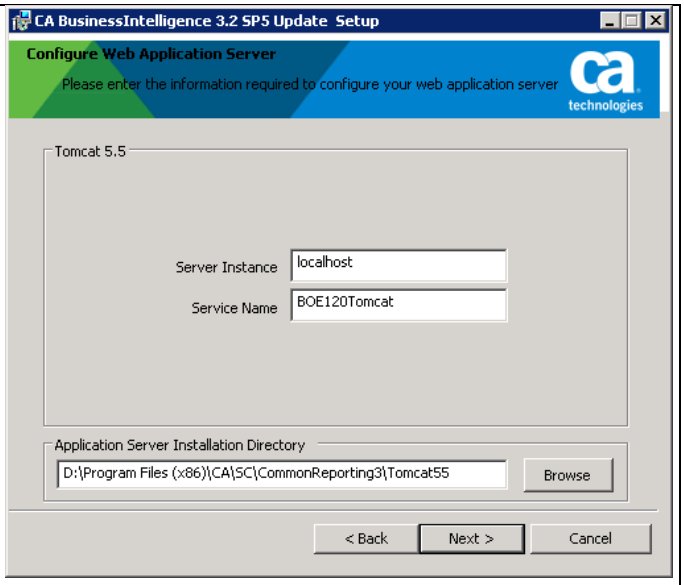
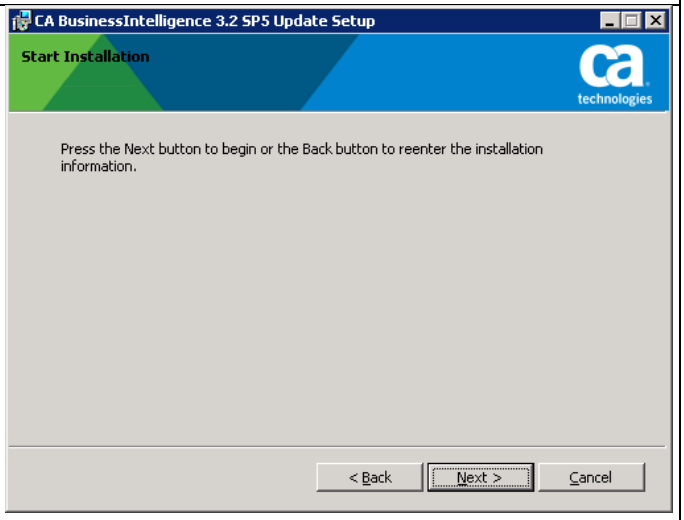
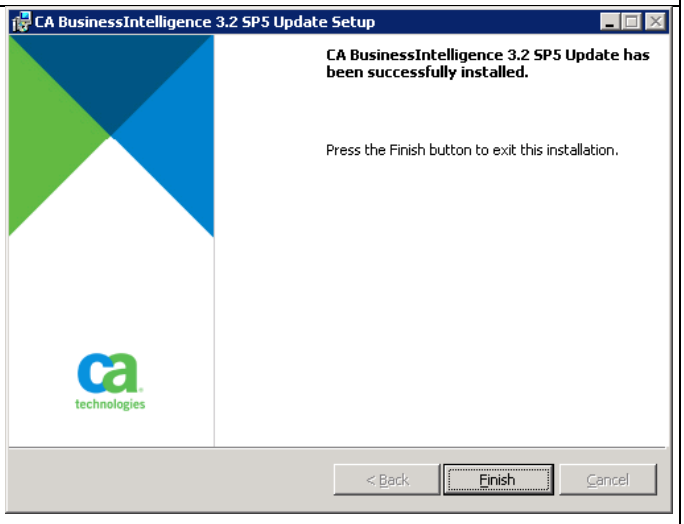
Copie el archivo en la siguiente ubicación D: \ Archivos de programa (x86) \ CA \ SC \ CommonReporting3 \ common \ 4.0 \ java \ lib	
Edite el CRConfig.xml	
Introduzca la ruta completa del archivo sqljdbc.jar copiado	

Reinicie todos los servidores en el gestor de configuración central	
Sigue el camino se muestra y ejecutar el setup.exe como administrador	
Haga clic en Aceptar	
Haga clic en Siguiente	

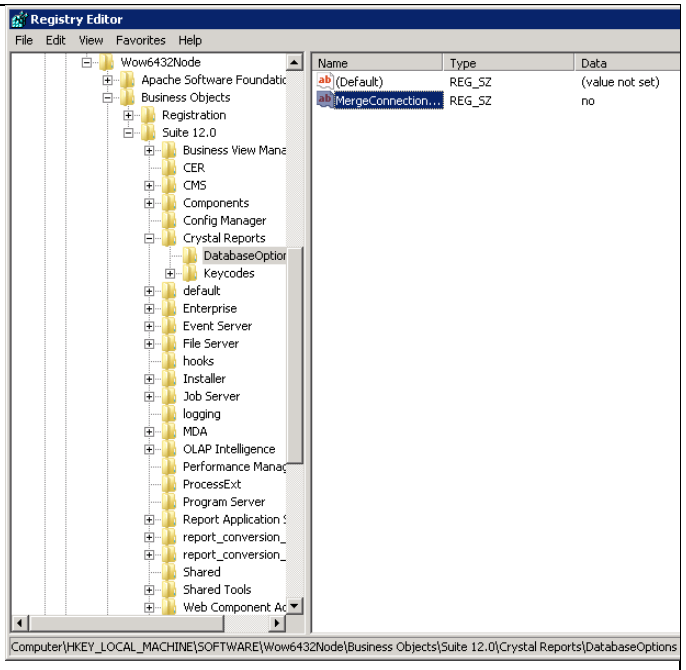
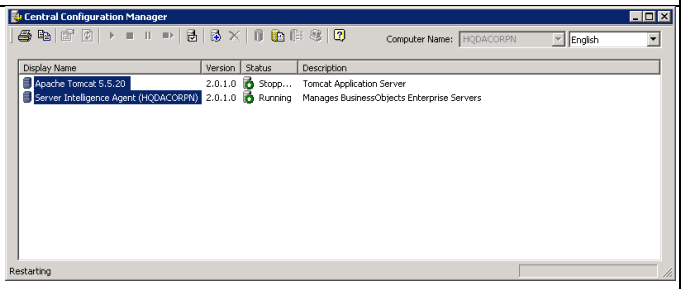
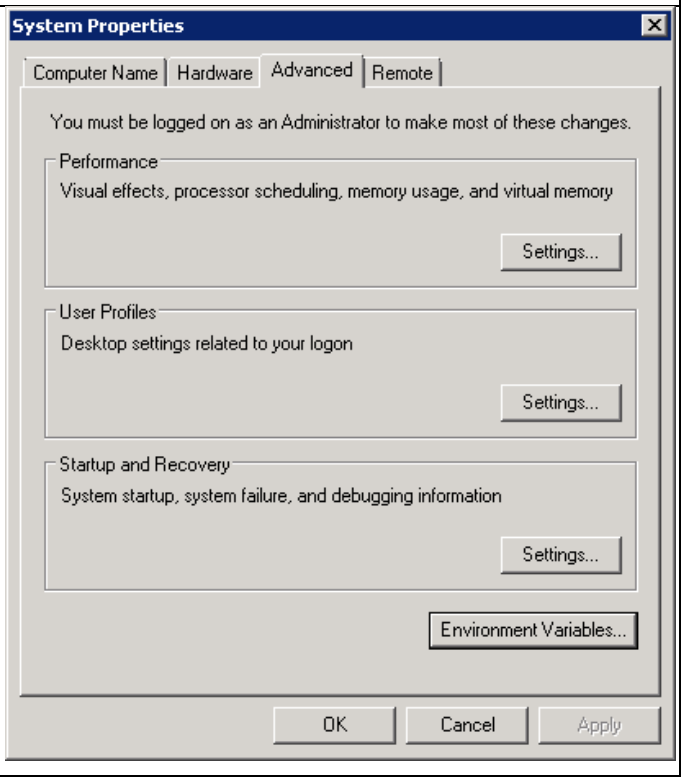
421

Acepte el acuerdo de licencia	
Introduzca la contraseña de administrador de CMS que se utilizó durante la instalación inicial	
Seleccione el botón de opción Sí	

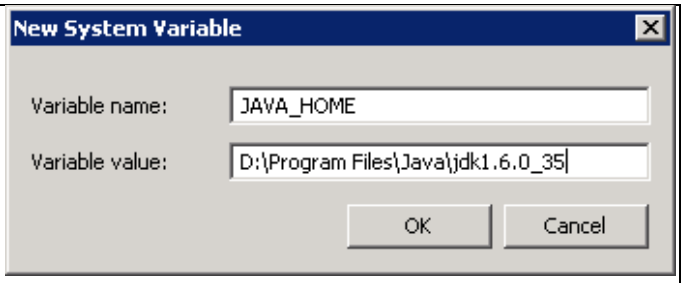
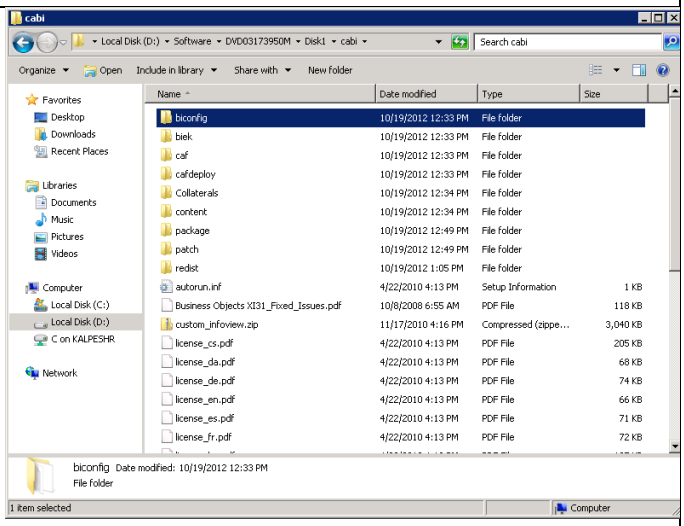
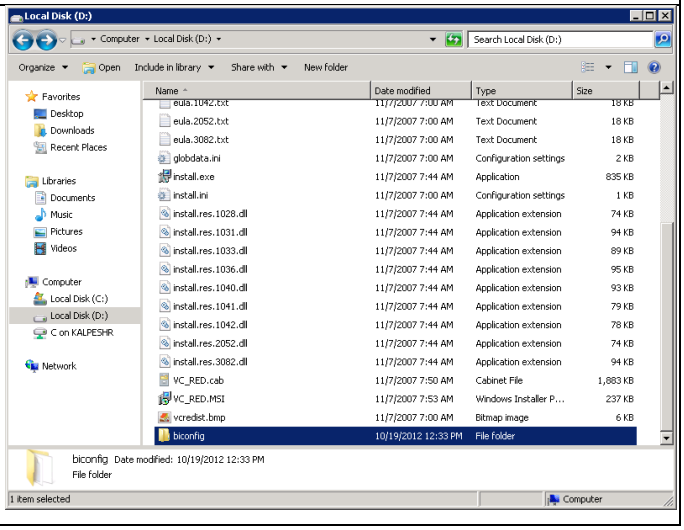
422

Verifique el camino es la unidad D	
Haga clic en Siguiente NOTA : Mantenga todos los servicios en CCM correr pero cerca de CCM	
Haga clic en Finalizar	

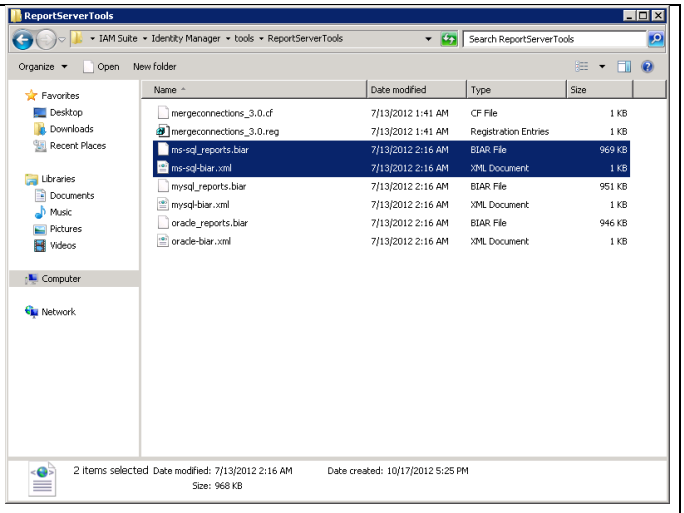
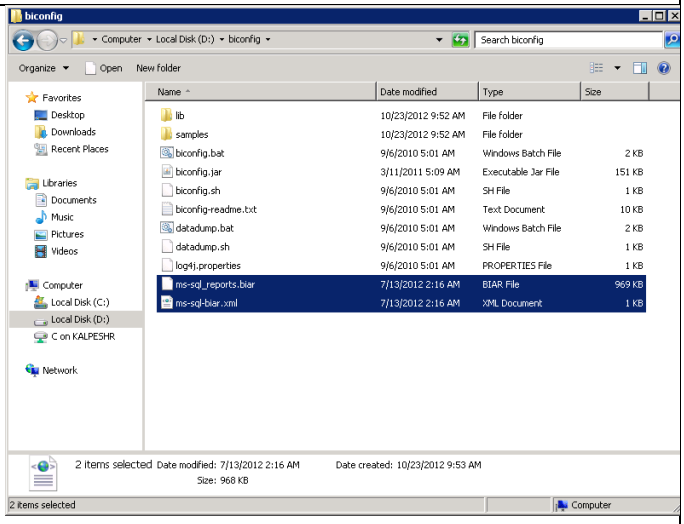
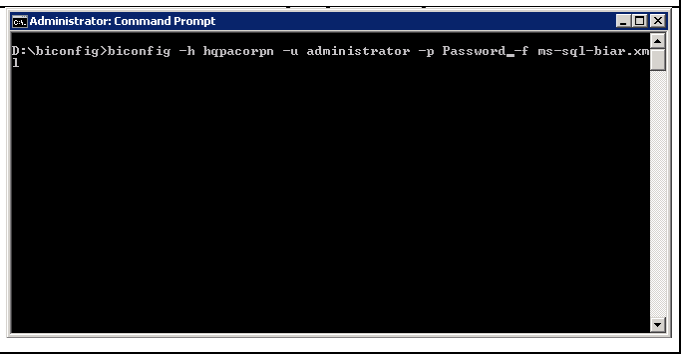
423

Ir a reg editar y navegar hasta la carpeta se muestra. Seleccione mergeconnectionproperties y cambie el valor a yes	
Reiniciar todo	
Establezca la variable de entorno JAVA_HOME	

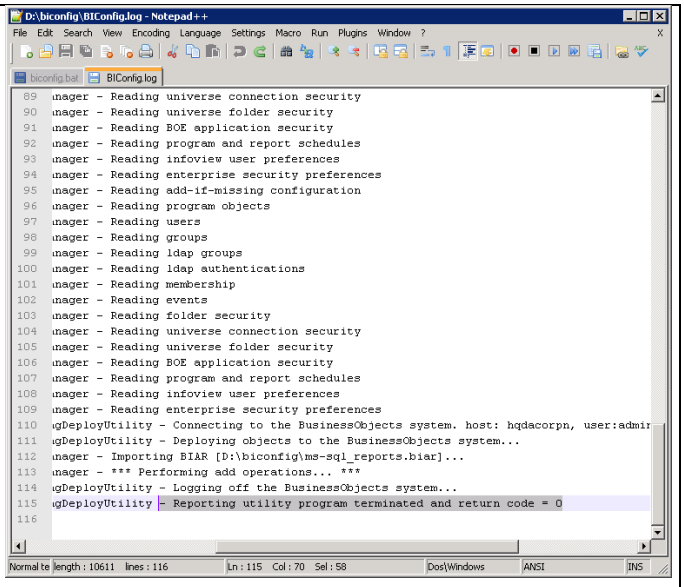
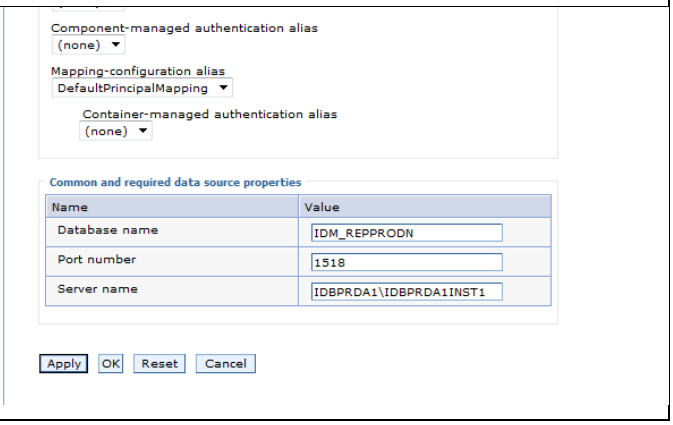
424

Cambiar ruta de acceso a la ubicación de JDK	
Copie sobre carpeta BIConfig desde el directorio se muestra a la raíz de la unidad D	
BIConfig en la raíz de la unidad D	

425

Ir al servidor WAS y copiar los dos archivos de las herramientas \ reportservertools \ carpeta	
Pegue los dos archivos copiados desde el servidor WAS a la carpeta BIConfig en la raíz de la unidad D	
Ejecute el comando como se muestra NOTA : muestra la contraseña incorrecta	

426

Compruebe que el archivo biconfig.log devuelve un 0 al final	
Inicie sesión en la consola de WAS y vaya a Recursos -> JDBC -> Fuentes de datos -> iam_im Informe instantánea Fuente de datos Compruebe la base de datos se define correctamente	

427

3 Configuración de un servidor web y un servidor de aplicaciones en maquinas separadas (a distancia)

En este tema se describe la instalación de un plug-in de servidor Web que WebSphere Application Server proporciona para comunicarse con una determinada marca de servidor web. Este procedimiento describe cómo instalar el servidor web y su plug-in de servidor Web para WebSphere Application Server en una máquina y la configuración del servidor de aplicaciones en el perfil predeterminado en otra máquina para comunicarse con el servidor Web.

Cuando existen varios perfiles, el programa de instalación de plug-ins configura sólo el perfil predeterminado. Ver configuración de plug-ins para una descripción del flujo de la lógica que determina cómo el instalador selecciona el perfil de configurar.

Si la familia de productos WebSphere Application Server es compatible con una marca particular de servidor Web, como IBM HTTP Server o Microsoft Internet Information Services (IIS), entonces su producto WebSphere Application Server proporciona un plug-in binario para el servidor Web que debe instalar.

Si la familia de productos WebSphere Application Server no proporciona un plug-in binario para una determinada marca de servidor web, el servidor web no es compatible. El propósito de la binario plug-in es proporcionar el protocolo de comunicación entre el servidor Web y el servidor de aplicaciones.

Supongamos que se crea un nuevo perfil. Supongamos también que usted desea utilizar un servidor Web. Debe instalar un nuevo servidor Web para el nuevo perfil y utilizar el asistente de instalación Plug-ins para instalar el módulo plug-in binario y configurar el servidor Web y el servidor de aplicaciones.

Si el servidor Web no está ya instalado, aún puede instalar los plug-ins para su uso futuro. Si el producto WebSphere Application Server no está instalado, aún puede instalar los plug-ins. Sin embargo, se recomienda que instale el servidor Web y el producto WebSphere Application Server antes de instalar los plug-ins para el servidor web compatible.

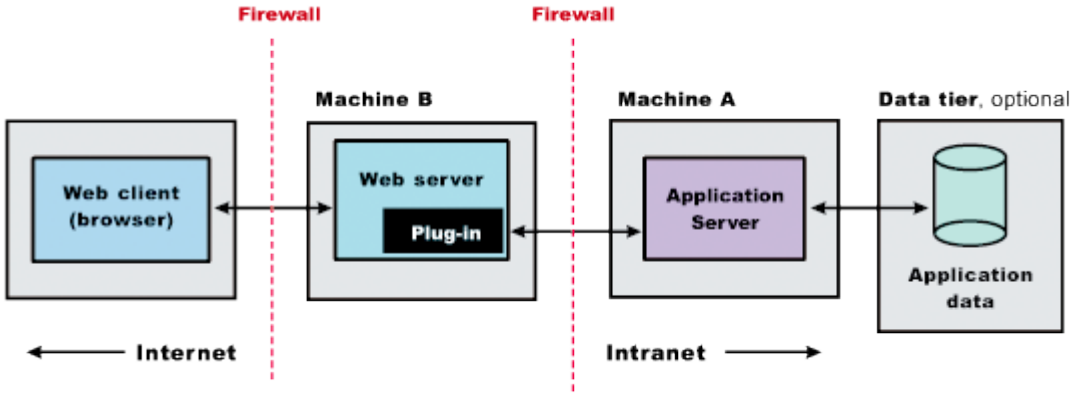
El asistente de instalación de plug-ins instala el módulo plug-in, configura el servidor Web para comunicarse con el servidor de aplicaciones y crea una definición de configuración del servidor Web en el servidor de aplicaciones, si es posible.

 428

Este procedimiento configura el perfil de servidor de aplicaciones que es el perfil predeterminado en la máquina. Existe una relación de uno a uno entre un servidor web y el servidor de aplicaciones .

En este tema se describe cómo crear la siguiente topologa(ver figura 11)

Figura 11



En este tema se describe la instalación de un servidor Web en una máquina y el servidor de aplicaciones en un equipo diferente . En esta situación, el asistente de instalación de plug- ins en una máquina no puede crear la definición de servidor Web en la configuración del servidor de aplicaciones en la otra máquina .

En tal caso , el asistente de instalación de plug- ins crea una secuencia de comandos en la máquina del servidor Web que se puede copiar a la máquina servidor de aplicaciones. Ejecute la secuencia de comandos en la máquina servidor de aplicaciones para crear la definición de configuración del servidor Web dentro de la configuración del servidor de aplicaciones .

Realice el siguiente procedimiento para instalar el plug-in y configurar el servidor Web y el servidor de aplicaciones.

1. Inicie sesión en el sistema operativo. Si va a instalar como no root o usuario no administrativo , entonces hay ciertas limitaciones. Consulte la documentación de la instalación no root para más información.

429

AIX | HP-UX | Linux | Solaris Además , seleccione un umask que permite al propietario de lectura / escritura a los archivos , y permite a otros a acceder a los mismos de acuerdo con la directiva del sistema imperante. Para raíz, se recomienda un umask de 022 . Para los usuarios que no sean root , una umask de 002 o 022 podría utilizarse , dependiendo de si los usuarios comparten el grupo.

Para verificar la configuración de la máscara U, emita el siguiente comando :

```
umask
```

Para establecer el valor de marcara U en 022 emita el siguiente comando:

```
umask 022
```

Windows Al instalar como usuario administrativo en un sistema operativo Windows, un servicio de Windows se crea automáticamente al iniciar automáticamente el servidor de aplicaciones . La cuenta de usuario de instalación debe tener los siguientes derechos avanzados de usuario :

o Actuar como parte del sistema operativo

o Iniciar sesión como un servicio

Por ejemplo , en algunos sistemas operativos de Windows , haga clic en Herramientas administrativas> Directiva de seguridad local > Los derechos de los usuarios de misiones para establecer las opciones avanzadas . Consulte la documentación del sistema operativo Windows para obtener más información .

Windows Si va a ejecutar el servidor de aplicaciones como un servicio de Windows, no instale desde un ID de usuario que contiene espacios. Un ID de usuario con espacios no se puede validar. Tal un ID de usuario no se le permite continuar la instalación. Para solucionar esta limitación, instale con un ID de usuario que no contenga espacios.

2. Instale WebSphere Application Server en la máquina A.

Lea el tema "Instalación del producto y el software adicional".

3.Instale IBM HTTP Server u otro servidor Web soportado en la máquina B.

10. Opcional: Cree un nuevo alias de host para el host virtual predeterminado.

Si ha configurado el servidor Web para utilizar un puerto distinto del puerto 80, deberá añadir un nuevo alias de host para ese puerto para el host predeterminado. Por ejemplo, cuando se ejecuta como no root, IBM HTTP Server está configurado con un valor de puerto predeterminado 8080.

5. Inicie el asistente de instalación de plug-ins en la máquina con el servidor Web.

Seleccione el asistente de instalación de plug-ins de la plataforma de lanzamiento o cambie los directorios al directorio de plugins en el disco del producto o en la imagen de instalación descargado y ejecute el comando de instalación.Desactive la casilla de verificación de la hoja de ruta o seleccione la casilla de verificación para ver la hoja de ruta, a continuación, haga clic en Siguiente.

Si no está seguro de que la instalación de escenarios para seguir, mostrar la hoja de ruta en su lugar. Imprimir y mantener la hoja de ruta como una visión práctica de los pasos de la instalación.

Presione Ctrl-P para imprimir la hoja de ruta si el navegador Web controles de navegación y la barra de menús no están presentes en la ventana del navegador que muestra la hoja de ruta de Plug-ins. Presione Ctrl-W para cerrar la ventana del navegador, si los controles de navegación y la barra de menús no se muestran. O cerrar la ventana del navegador con el control de la ventana en la barra de título.

1. Lea el acuerdo de licencia y acepte el acuerdo de que si está de acuerdo con sus términos. Haga clic en Siguiente cuando haya terminado.

2. Si el sistema no pasa los requisitos de verificación, detener la instalación, corregir cualquier problema, y reinicie la instalación. Si el sistema pasa los requisitos previos de verificación, haga clic en Siguiente.

431

Busque el archivo de registro correspondiente para obtener información sobre los requisitos previos que faltan:

o Si usted deja la instalación, consulte el archivo temporaryPluginInstallLog.txt en el directorio temporal del usuario que ha instalado los plug-ins. Por ejemplo, el archivo /tmp/temporaryPluginInstallLog.txt podría existir si el usuario root instalado los plug-ins en un sistema operativo como AIX o Linux.

o Si usted continúa la instalación a pesar de las advertencias acerca de los requisitos previos que faltan, consulte las plugins_root / logs / install / archivo log.txt después de la instalación se haya completado.

Lea el tema "Solución de problemas de instalación" para obtener más información acerca de los archivos de registro.

9. Seleccione el tipo de servidor Web que está configurando y haga clic en Siguiente.La instalación de paneles asistente Plug-ins le pide que identifique los servidores web para configurar. En realidad, usted puede seleccionar sólo un servidor Web cada vez que se ejecuta el asistente de instalación de plug-ins.

Deje de cualquier servidor Web mientras está configurando ello. Un paso adelante en el procedimiento le indica que inicie el servidor Web a medida que comienza la prueba servlet snoop.

Si selecciona la opción de identificación del servidor Web Ninguno marcado, el servidor Web instala los plug-ins binarios, pero no configura el servidor Web.

10. Seleccione la máquina del servidor Web (remoto) y haga clic en Siguiente.

11. Acepte la ubicación predeterminada para el directorio raíz de la instalación de los plug-ins. Haga clic en Siguiente.

Puede escribir otro nuevo directorio o haga clic en Examinar para seleccionar un directorio vacío. La ruta de acceso completa identifica el directorio raíz de instalación de plug-ins.

La ubicación predeterminada se muestra en las convenciones Directory.

Restricción:

El directorio de instalación no puede contener caracteres no admitidos. Ver "Los nombres de objeto: lo que la cadena de nombre no puede contener" para obtener más información.

Existe una posibilidad de que el servidor Web puede ejecutarse en una plataforma que WebSphere Application Server no admite.

12.Haga clic en buscar y seleccione el archivo de configuración del servidor Web , compruebe que el puerto del servidor Web es correcta y haga clic en Siguiente cuando haya terminado .

Seleccione el archivo y no sólo el directorio del archivo . Algunos servidores web tienen dos archivos de configuración y requieren que buscar cada archivo.

La siguiente lista muestra los archivos de configuración para los servidores Web compatibles :

Apache HTTP Server

apache_root / config / httpd.conf

Domino Web Server

names.nsf y Notes.jar

El asistente solicita el archivo notes.jar . El nombre real es Notes.jar .

El asistente de instalación de plug-ins verifica que los archivos existen , pero el asistente no valida cualquier archivo .

IBM HTTP Server

Microsoft Internet Information Services (IIS)

El asistente de instalación de plug-ins puede determinar los archivos correctos para editar .

Sun Java System Web Server (anteriormente Sun ONE Web Server y iPlanet Web Server) versión 6.0 y posteriores

obj.conf y magnus.conf

El asistente muestra un panel de nomenclatura para el apodo de la definición de servidor Web .13. Especifique un apodo para el servidor Web.

Haga clic en Siguiente cuando haya terminado .

El asistente utiliza el valor a las carpetas de configuración de nombre en el directorio raíz de instalación de plug-ins. El asistente también utiliza el nombre de la secuencia de comandos de configuración para el servidor de aplicaciones para nombrar la definición de servidor Web.

Si el perfil de servidor de aplicaciones ya tiene una definición de servidor Web , elimine la definición del servidor Web antes de continuar. Utilice los siguientes comandos para eliminar la

definición de servidor Web:$AdminTask deleteServer { -serverName webserver1 -nodeName webserver1_node }

$AdminTask removeUnmanagedNode { -nodeName webserver1_node }

$AdminConfig save

En estos comandos, webserver1 es el nombre del servidor Web .

14. Acepte la ubicación predeterminada para el archivo plugin- cfg.xml que el asistente crea en el equipo servidor Web , haga clic en Siguiente .

Puede escribir un cambio en el valor o haga clic en Examinar para seleccionar un archivo en otra ubicación . Si usted no acepta la ubicación predeterminada, debe existir el archivo plugin- cfg.xml .

15. Identificar el nombre de host o la dirección IP de la máquina A, que es la máquina servidor de aplicaciones, haga clic en Siguiente.

16. Examine el panel de resumen. Haga clic en Siguiente cuando haya terminado.

El panel le notifica que tiene pasos manuales para realizar para completar la instalación y configuración. El tipo de servidor Web, el apodo del servidor Web, y la ubicación de las pantallas del plugin cfg.xml de archivos en el panel.

El asistente de instalación de plug-ins crea el guión configureWeb_server_name en el directorio plugins_root / bin / en la máquina B (la máquina con el servidor web).

El asistente de instalación de plug-ins también crea el archivo plugin-cfg.xml en el directorio / config / nombre_servidor_Web plugins_root.

El servidor Web lee el archivo plugin-cfg.xml para determinar las aplicaciones que el servidor de aplicaciones en la máquina A puede servir al servidor Web en la máquina B. Cada vez que los cambios de configuración, el servidor de aplicaciones regenera el archivo. Cuando se produce la regeneración, propagar, o copiar el archivo plugin-cfg.xml real de la máquina servidor de aplicaciones de la máquina del servidor Web. Puede propagarse automáticamente el archivo al producto IBM HTTP

Server.

17. Haga clic en Siguiente en el panel de resumen previo a la instalación para comenzar la instalación o haga clic en Atrás para cambiar las características de la instalación.

El panel especifica el directorio de instalación de plug-ins de la raíz, la función de plug-ins de servidor Web y el tamaño del disco del código que se instala cuando se hace clic en Siguiente.

18. Después de que el asistente instala el código y crea el programa de desinstalación , examine el panel de resumen posterior a la instalación . Haga clic en Siguiente cuando haya terminado para mostrar la hoja de ruta de instalación de plug-ins .

El asistente de instalación de plug-ins instala el módulo plug-in binario. En un sistema Linux , por ejemplo , la instalación crea el directorio plugins_root . El directorio / config / nombre_servidor_Web plugins_root contiene el archivo plugin- cfg.xml .

El asistente muestra el nombre y la ubicación del script de configuración y el archivo plugin-cfg.xml . El asistente también muestra el tipo de servidor Web que se configura y el apodo del servidor Web .

Si se produce un problema y la instalación no se realiza correctamente , examine los registros en el directorio plugins_root / logs . Corrija cualquier problema y volver a instalar .

19. Cierre la hoja de ruta y haga clic en Finalizar para salir del asistente.

Los archivos de registro de la instalación están en la plugins_root / logs directorio de instalación /

.

17.1.1 Complete la configuración de IIS (7.0)

Antes de iniciar este procedimiento , compruebe que está utilizando una versión 6.1.0.9 o posterior del servidor Web plug-in. Las versiones anteriores del plug-in no son compatibles con el sistema operativo Windows Server 2008 .

Sigue estos pasos:

1. Instale la versión 7.0 de IIS con la versión de IIS 6.0 componentes de compatibilidad de

gestión necesarias . Componentes Versión IIS 6.0 Compatibilidad con la administración no se instalan por defecto.

A. Complete los siguientes pasos para que aparezca la ventana de Administrador de servidores en Windows Server 2008 :

o Haga clic en Inicio, Herramientas administrativas , Gerentes Server.

o Haga clic en Acción, para agregar funciones , y luego haga clic en Siguiente .

- En la página Seleccionar funciones de servidor , active la función de servidor web (IIS) y , a continuación, haga clic en Siguiente .
- Si un mensaje para el Windows Process Activation Service función muestra, haga clic en Agregar características, en Siguiente.
- Haga clic en Siguiente en la página de introducción de IIS.

B. Cuando el papel window displays, compruebe que están seleccionadas las opciones siguientes, además de las opciones por defecto que ya están seleccionados.

- Internet Information Server: Herramientas de Gestión
- la versión de IIS 6.0 Compatibilidad de gestión: La versión de IIS 6.0 Management Console, Versión IIS 6.0 Herramientas de scripting, versión IIS 6.0 Compatibilidad de WMI, y la compatibilidad de IIS metabase
- desarrollo de aplicaciones: Extensiones ISAPI, filtros ISAPI

C. Haga clic en Siguiente para activar las opciones seleccionadas y, a continuación, haga clic en Instalar en la siguiente ventana para realizar la instalación.

D. Cuando la instalación finalice, haga clic en Cerrar en la ventana Resultados de la instalación.

2. Entrar en la consola de administración del gestor de despliegue.

3. Abra el símbolo y el Comando vaya a: \ Archivos de programa \ IBM \ WebSphere \ AppServer \ profiles \ AppSrv01 \ bin.

 437

4. Ejecutar este comando: GenPluginCfg.bat.

El archivo plugin-cfg.xml se encuentra en C: \ Archivos de programa \ IBM \ WebSphere \ AppServer \ profiles \ AppSrv01 \ config \ cells.

5. Cree un directorio en C: \, por ejemplo, c: \ plugin.

6. Copie el archivo plugin-cfg.xml en el directorio c: \ directorio de plugins.

7. Copia iisWASPlugin_http.dll (ubicado en el servidor IIS) presentar al directorio c: \ plugin.

8. Seleccione Inicio, Todos los programas, Herramientas administrativas, Internet Information Services (IIS) en un sistema operativo Windows Server 2008. Esta acción inicia la aplicación de IIS y crea un nuevo directorio virtual para la instancia de sitio Web. Estas instrucciones asumen que está utilizando el sitio Web predeterminado.

9. Expanda el árbol de la izquierda hasta que vea el sitio Web predeterminado.

10. Haga clic en Sitio Web predeterminado, Agregar directorio virtual para crear el directorio con una instalación predeterminada.

1. 11. Introduzca sePlugins en el campo Alias de la ventana Directorio Alias Virtual del Asistente para crear un directorio virtual.12. Vaya a la c: \ directorio de plugins en el campo Ruta de Física de la ventana Directorio de contenido del sitio Web del asistente, y luego haga clic en Aceptar. Por ejemplo, seleccione la carpeta C: \ plugin.

2. 13. Haga clic en el botón Probar configuración. Si la prueba de configuración falla, puede cambiar los permisos del directorio físico. Alternativamente, seleccione Conectar como, y dejar que IIS conectar como una cuenta de usuario de Windows que tenga autoridad para archivos de esa ruta física.

3. 14. Haga clic en Aceptar para agregar el directorio virtual sePlugins a su sitio Web predeterminado.

4. 15. En el árbol de navegación, seleccione el directorio virtual sePlugins que acaba de crear.

 438

5. 16. En el panel Características, haga doble clic en Asignaciones de controlador y, a continuación, haga clic en Editar permisos de características en el panel de acciones.

6. 17. Seleccione Guión y Ejecutar, si no están ya seleccionadas.

7. 18. Haga clic en Aceptar.

8. 19. Volver a la ventana del Administrador de IIS y expanda la carpeta Sitios Web en el árbol de navegación de la izquierda de la ventana.

9. 20. Seleccione Sitio Web predeterminado en el árbol de navegación.

10. 21. Agregue la interfaz de programación de aplicaciones de Servicios de Internet (ISAPI) filtrarse en la configuración de IIS.

11. Por defecto el panel Propiedades del sitio Web, complete los siguientes pasos:

1. Haga doble clic en la ficha Filtros ISAPI.

2. Haga clic para abrir el cuadro de diálogo Agregar / Editar propiedades de filtro.

3. Introduzca iisWASPlugin en el campo Nombre del filtro.

4. Haga clic en Examinar para seleccionar el plug-in de archivo ubicado en el directorio c: Plugin directorio \ \ iisWASPlugin_http.dll.

5. Haga clic en Aceptar para cerrar la ventana de diálogo Agregar / Editar propiedades de filtro.

22. En el árbol de navegación, seleccione el nodo de servidor de nivel superior.

23. Por las características del panel, haga doble clic en Restricciones de ISAPI y CGI, y luego, en el panel de acciones, haga clic en Agregar.

Para determinar el valor de especificar para la propiedad Path ISAPI o CGI, busque y seleccione el mismo plug-in de archivos que seleccionó en el paso anterior. Por ejemplo: c: \ plugin \ iisWASPlugin_http.dll

 439

Introduzca WASPlugin en el campo Descripción, seleccione Permitir ruta extensión a ejecutar y, a continuación, haga clic en Aceptar para cerrar las Restricciones de ISAPI y CGI ventana de diálogo.

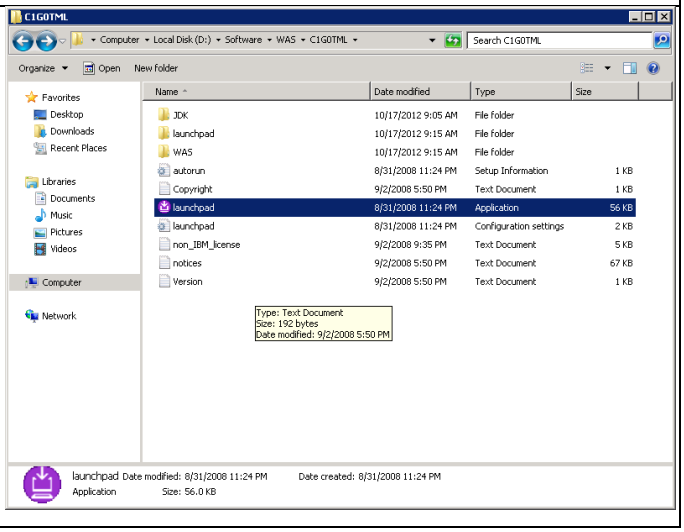
24. Crear el nuevo archivo con el nombre "plugin-cfg.loc" en zona c: \ plugin. Establezca el valor en el archivo plugin-cfg.loc a la ubicación del archivo de configuración. La ubicación predeterminada es C: \ plugin \ plugin-cfg.xml.

25. Reiniciar IIS versión 7.0 y su perfil de WebSphere Application Server.

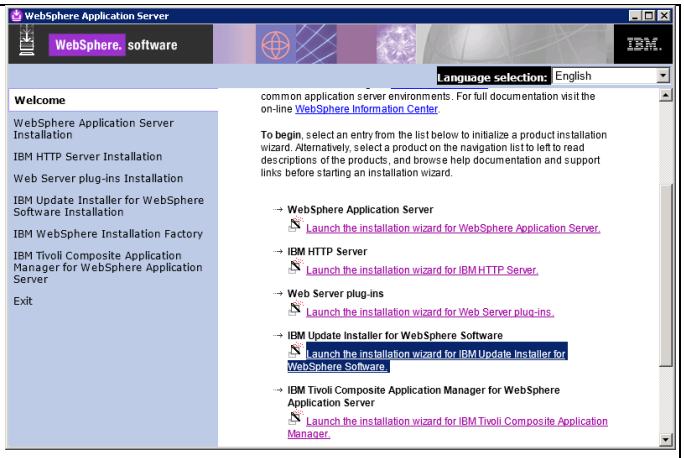
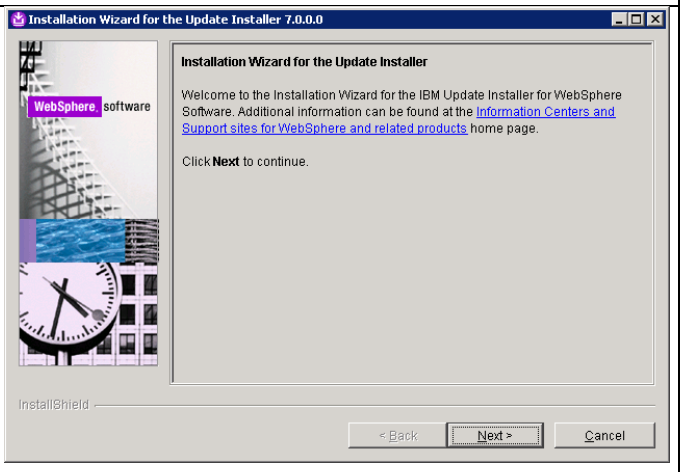
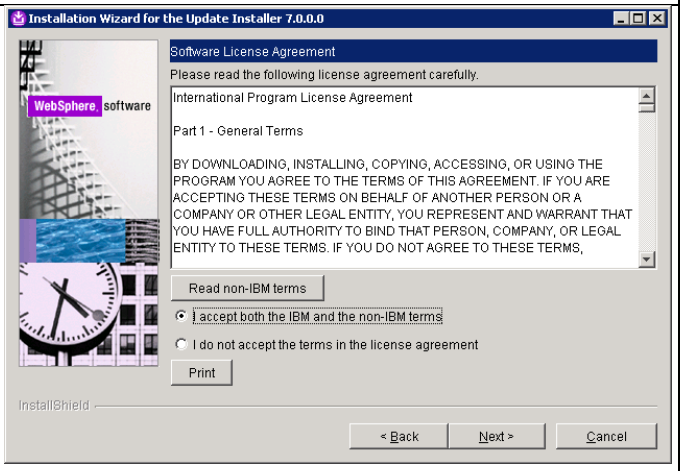
26. Verifique que snoop se está ejecutando.

17.1.2 actualización se Enchufe

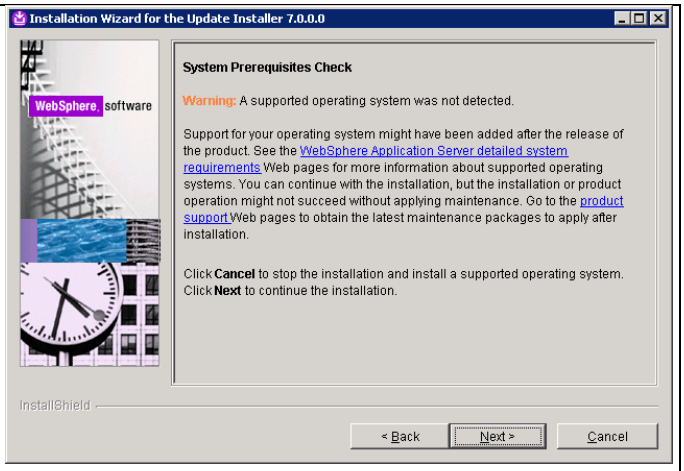
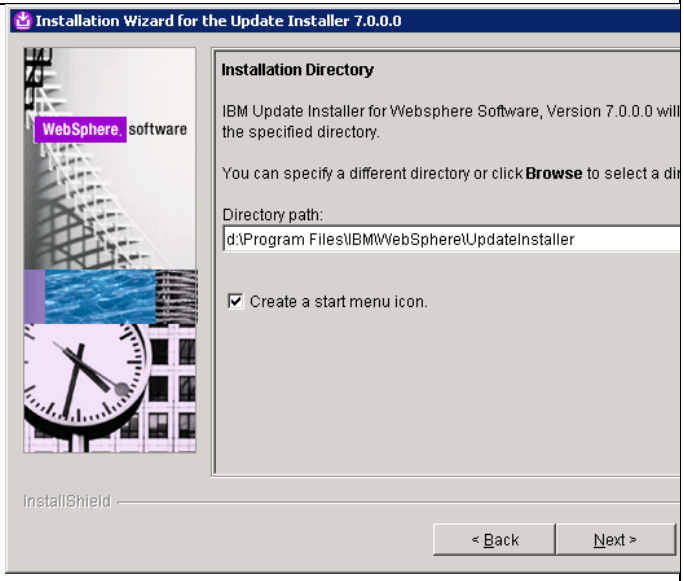
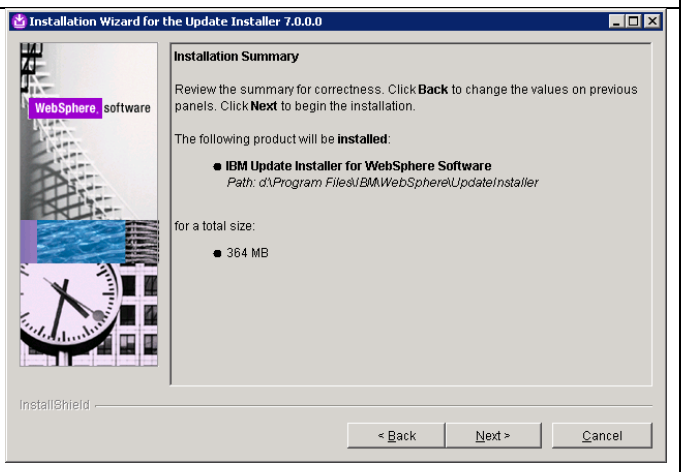
Los siguientes procedimientos explican los pasos que se requieren para instalar el plug WAS en el servidor IIS

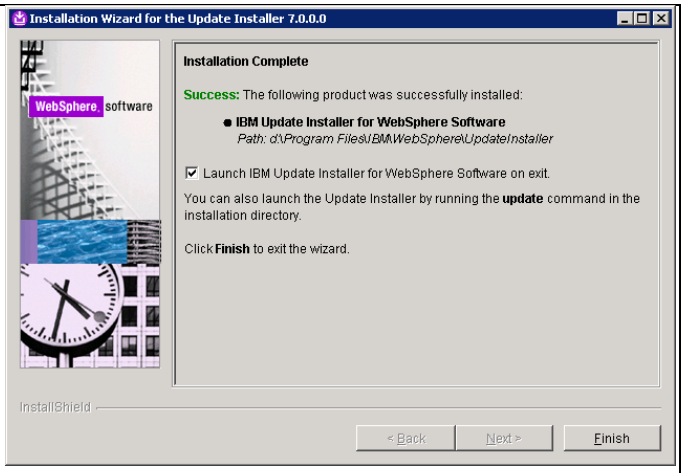
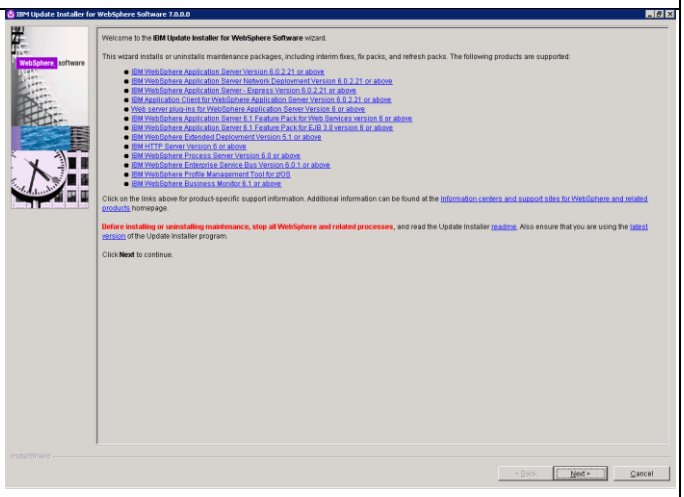
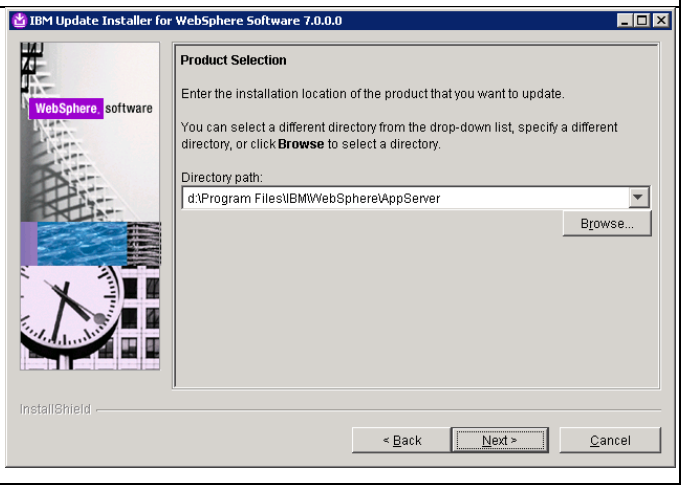
Instalar WAS Plug in	
Run the Launchpad	

440

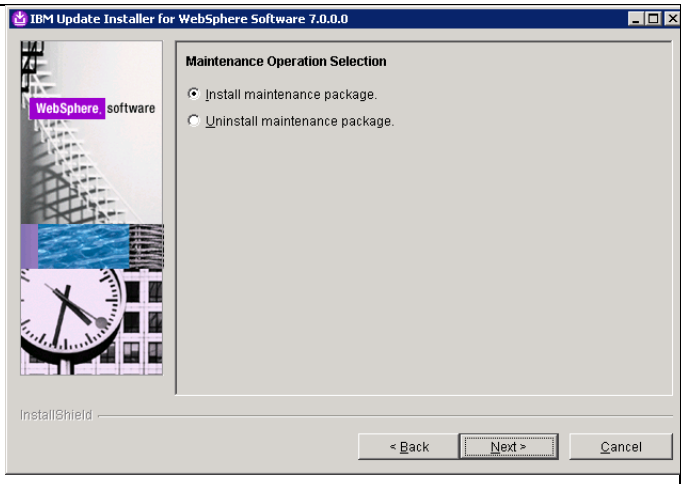
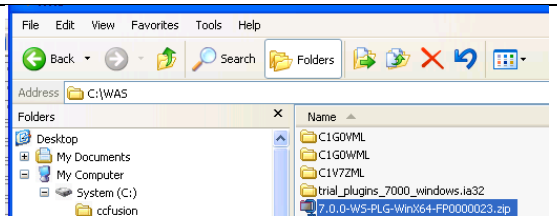
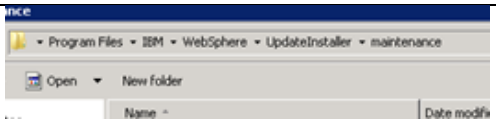
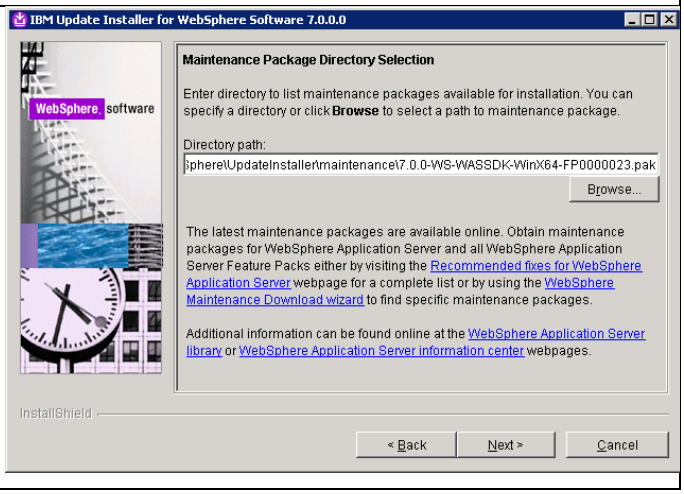
En el Área de ejecución , haga clic en el enlace para instalar la instalación de la actualización	
Haga clic en Siguiente	
Aceptar el acuerdo de la licencia	

441

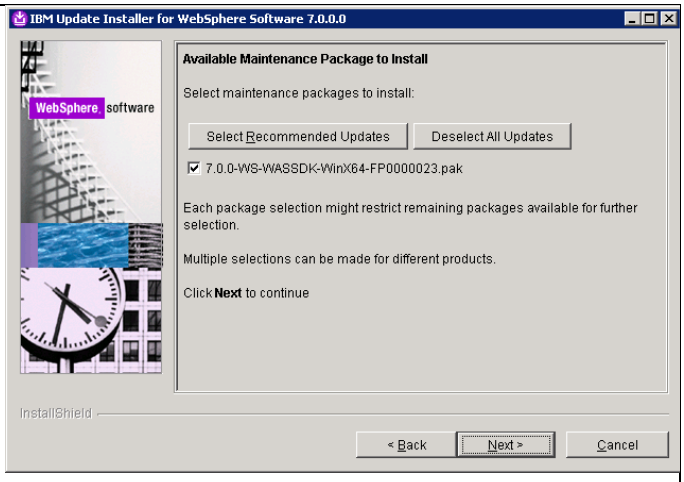
Haga clic en Siguiente	
Especifique la ubicación de la WAS Plugin NOTA : Estaba en C	
Revise el resumen de la instalación	

Después de la instalación de lanzar la actualización	
Haga clic en Siguiente	
Compruebe la ubicación del WAS Enchufe NOTA : Path se muestra en la pantalla es incorrecta	

443

Seleccione el paquete de mantenimiento de instalación	
Busque el archivo 7.0.0-WS-PLG-WinX64-FP0000023.zip y cambie la extensión zip un .pak	
Copie el archivo a la carpeta de mantenimiento instalador de actualizaciones	
Haga clic en siguiente en la pantalla del instalador NOTA : archivo incorrecto se muestra	

444

Compruebe que el enchufe en el archivo de fixpack está marcada. NOTA : Paquete incorrecta se muestra en la foto	
Verifique el resumen de la instalación y haga clic en Siguiente. Esto completará la actualización fixpack	
Vaya a C: \ Archivos de programa \ IBM \ WebSphere \ Plugins \ bin y sonó la versioninfo.bat para verificar la versión de fixpack	

22 Pasos de integración Cambio de punto final

Instale el agente remoto de Exchange 2007 o 2010 en cada logrado Exchange 2007 o 2010 Server que aloja la función de buzón de Exchange.

Se requieren siguientes pasos de configuración para el intercambio

Pasos Pre-requisitos

Cuenta AD 1. w / contraseña como servicio de intercambio cuenta con los siguientes privilegios / Exchange 2010 papeles recomienda:

• Para mover buzón, Derechos del buzón (Permisos de acceso completa) Disponer de la función Administrador de la organización

• Para el resto de Tareas de Exchange (no es necesario si un miembro de Administrador de la organización de Exchange) proporcionar destinatarios de Exchange Administradores de papel

• grupo de administradores locales y también el grupo \ Administradores de dominio orden interna a la cuenta del BID \ svc_eta_xchg AD

2. A raíz de los puertos de firewall deben estar abiertos en el caso de AD, Exchange y IDM existe en VLAN separadas / subredes

• Cambio de nombre FQDN del servidor

• Puerto 4104 y 4105 de los servidores de aprovisionamiento Prod y Exchange Server (s) donde está instalado el agente de cambio de IDM. Servidor de Exchange debe "vivir" cerca del punto final de Active Directory primaria que usted definir este Exchange Server como la puerta de enlace.

• Puertos 3268/3269 y 445 entre los servidores de aprovisionamiento y AD servidor de catálogo global (necesidad de identificar Servidor Catálogo AD Global (s), esto es generalmente el controlador de dominio)Pasos de instalación / configuración

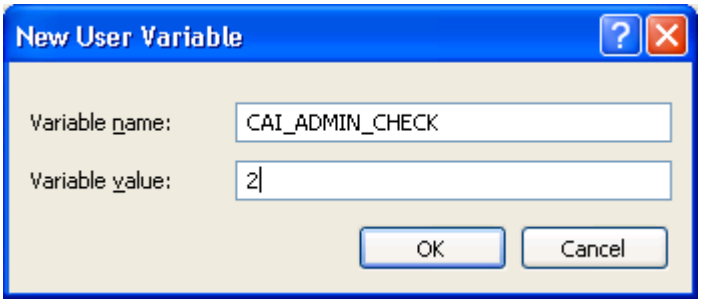
1. Verifique que el acceso a la ubicación de la carpeta Exchange20072010

2. Inicie la sesión como svc_eta_xchg (o equivalente)

- 3. Instale el Agente IdM en el servidor de Exchange
- a. Ejecute setup.exe
- b . Elige lengua
- c . Haga clic en Aceptar para instalar C ++ Feature Pack
- d. Haga clic en Siguiente en la pantalla de bienvenida
- e. Acepte la licencia

- f . Seleccione la carpeta de instalación
- g . Haga clic en instalar
- h . Haga clic en Finalizar después de exitosa instalación
- i. Reinicie el servidor
- Instalar pasos de configuración en Exchange Server

3. Agregue la siguiente variable de entorno



4. Vertifique la entrada de la ruta de registro a continuación se establece en 60 en la prueba pero 1 en la producciónn

[HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager] "Ex2k7AgentTimeout"=60

5. Ejecutar cafthost -l en un símbolo del sistema para ver si hay servidores de la lista

6. Eliminar entrites servidor anterior utilizando cafthost -d hqdaprov03.idb.iadb.org

7. Escribir un servidor de aprovisionamiento mediante la ejecución cafthost -a hqdaprovn.idb.iadb.org (nombre del servidor de prueba se muestra)

(El comando anterior se suma el aprovisionamiento de entrada de nombre de servidor en "C: \ Archivos de programa (x86) \ CA \ SharedComponents \ CAM \ cafthost.cfg " y verificar esto)

8. Servicio de levas de reinicio mediante comandos

o camclose

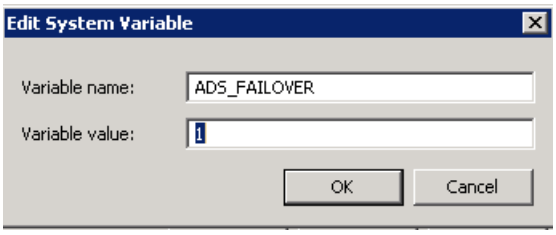
o inicio de leva

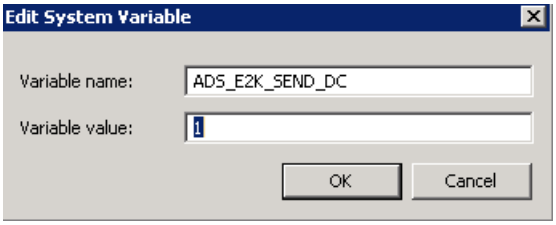
9. Ejecutar services.msc

10. Verifique que el servicio de CA Message Queue Server se ejecuta como cuenta el " BID \ svs_eta_xchg " . Si no lo es, cambiarlo

El servidor de aprovisionamiento ,

11. Agregar siguientes variables de entorno





12. El punto final de AD , ver si pestañas Exchange están habilitados y el servidor de puerta de

enlace correcto es seleccionado junto con otros ajustes de cambio

13. En los servidores de aprovisionamiento , configure la cuenta de que el servicio se ejecuta bajo IM_CCS requiere administrador de dominio (siempre) y Administrador de destinatarios de Exchange (sólo si se ejecuta Exchange 2007/2010) .

18. Apéndice

Instalación 18.1 Identidad Minder PatchEl propósito de esta revisión es hacer frente a un problema de seguridad que se encuentra en IdentityManager r12 , r12.5 y r12.6 .

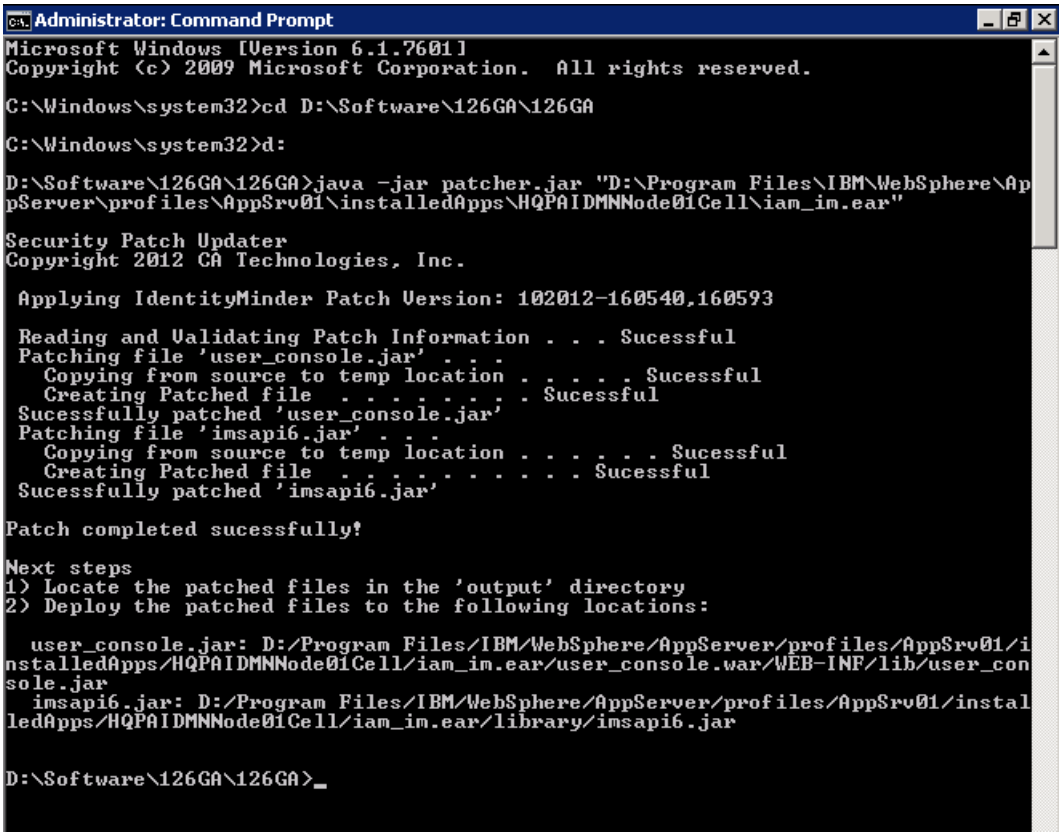
Para instalar el parche siga los procedimientos descritos a continuación .

• Vaya a D: \ Software \ 126GA \ 126GA en una ventana de símbolo del sistema

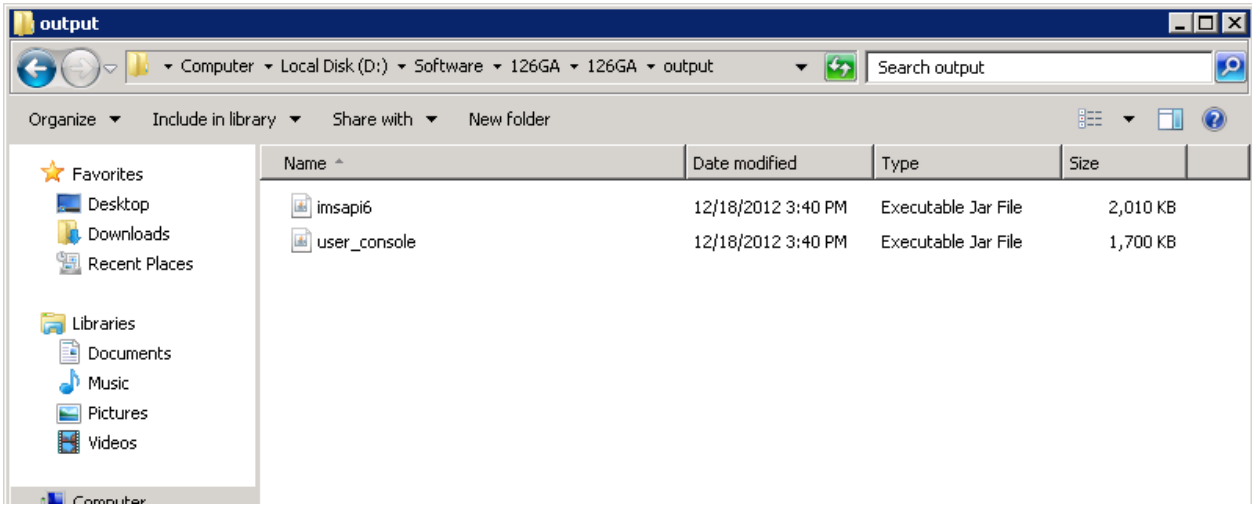
• Ejecute los siguientes comandos

Patcher.jar Java -jar "D: \ Archivos de programa \ IBM \ WebSphere \ AppServer \ profiles \ AppSrv01 \ installedApps \ HQDAIDMNNode01Cell \ iam_im.ear "

449

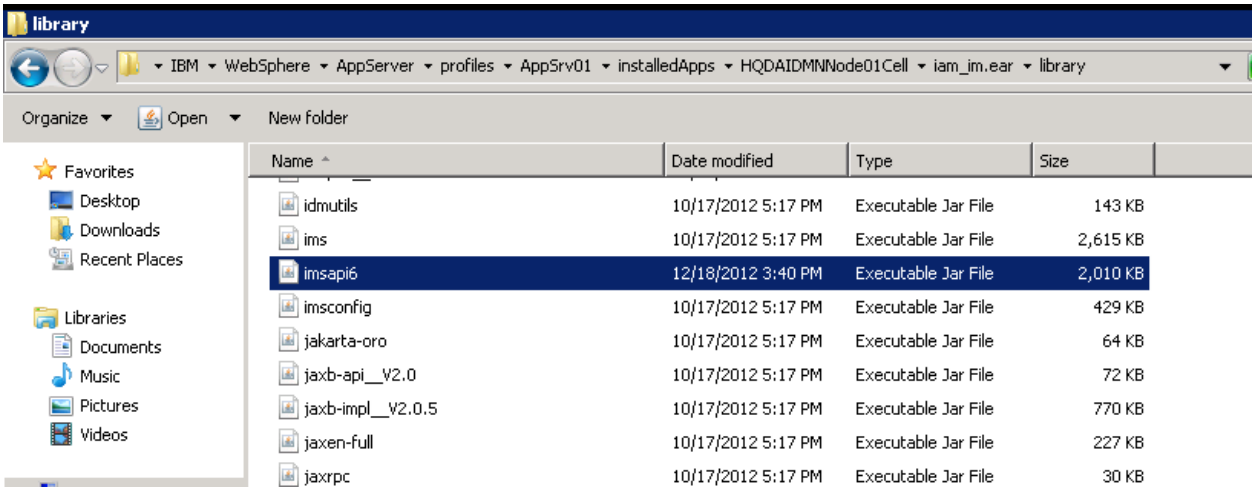


- Upon completion two files will be created in the output folder created in the 126GA



- Copy the imsapi6 jar file to the following location (overwrite the original):

D:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\HQDAIDMNNode01Cell\iam_im.ear\library



- Copy the user_console jar file to the following location (overwrite the original):

D:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\HQDAIDMNNode01Cell\iam_im.ear\user_console.war\WEB-INF\lib

451

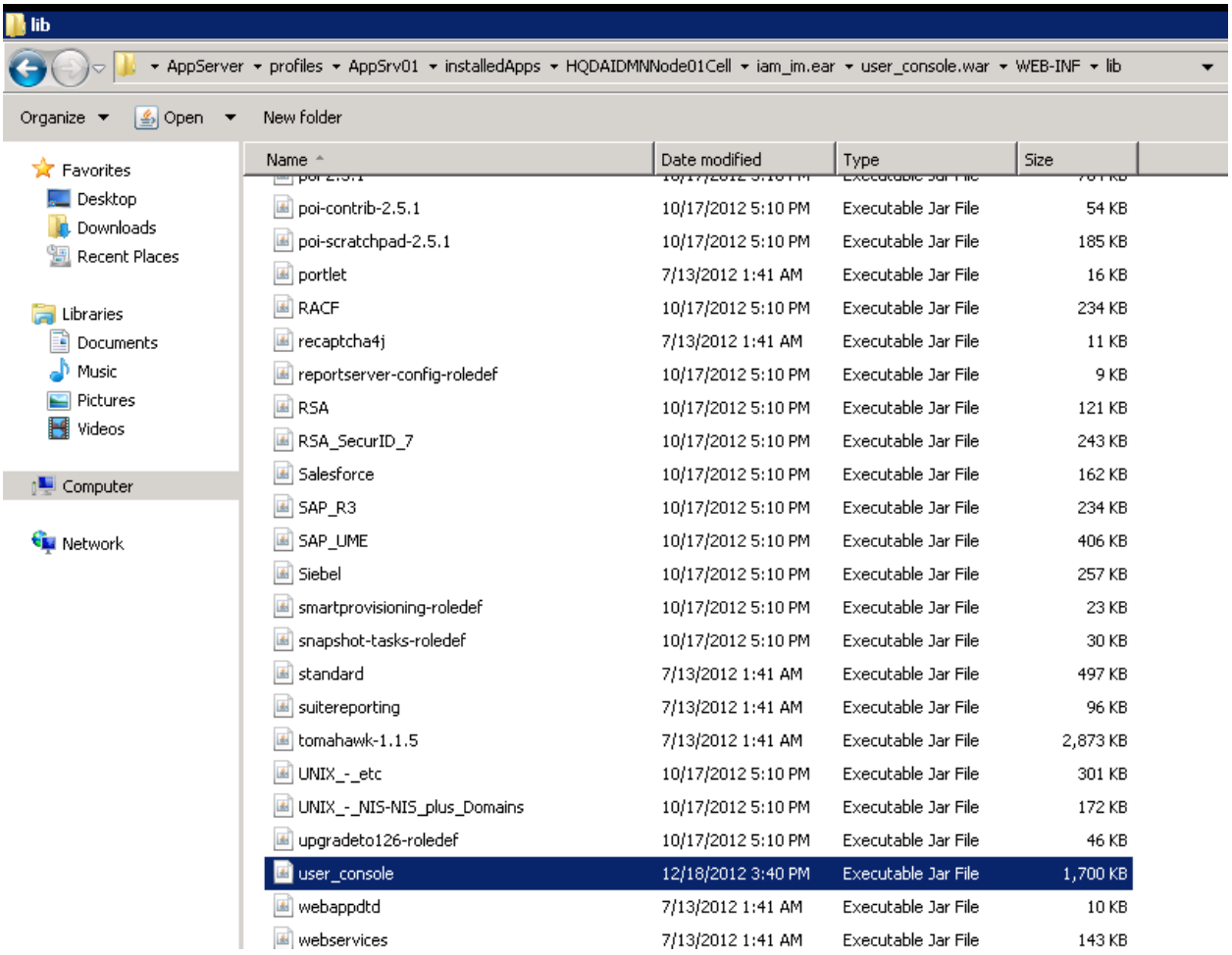

lib
AppServer ▸ profiles ▸ AppSrv01 ▸ installedApps ▸ HQDAIDMNNode01Cell ▸ iam_im.ear ▸ user_console.war ▸ WEB-INF ▸ lib
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
poi-contrib-2.5.1 10/17/2012 5:10 PM Executable Jar File 54 KB
poi-scratchpad-2.5.1 10/17/2012 5:10 PM Executable Jar File 185 KB
portlet 7/13/2012 1:41 AM Executable Jar File 16 KB
RACF 10/17/2012 5:10 PM Executable Jar File 234 KB
recaptcha4j 7/13/2012 1:41 AM Executable Jar File 11 KB
reportserver-config-roledef 10/17/2012 5:10 PM Executable Jar File 9 KB
RSA 10/17/2012 5:10 PM Executable Jar File 121 KB
RSA_SecurID_7 10/17/2012 5:10 PM Executable Jar File 243 KB
Salesforce 10/17/2012 5:10 PM Executable Jar File 162 KB
SAP_R3 10/17/2012 5:10 PM Executable Jar File 234 KB
SAP_UME 10/17/2012 5:10 PM Executable Jar File 406 KB
Siebel 10/17/2012 5:10 PM Executable Jar File 257 KB
smartprovisioning-roledef 10/17/2012 5:10 PM Executable Jar File 23 KB
snapshot-tasks-roledef 10/17/2012 5:10 PM Executable Jar File 30 KB
standard 7/13/2012 1:41 AM Executable Jar File 497 KB
suitereporting 7/13/2012 1:41 AM Executable Jar File 96 KB
tomahawk-1.1.5 7/13/2012 1:41 AM Executable Jar File 2,873 KB
UNIX_-_etc 10/17/2012 5:10 PM Executable Jar File 301 KB
UNIX_-_NIS-NIS_plus_Domains 10/17/2012 5:10 PM Executable Jar File 172 KB
upgradeto126-roledef 10/17/2012 5:10 PM Executable Jar File 46 KB
user_console 12/18/2012 3:40 PM Executable Jar File 1,700 KB
webappdtd 7/13/2012 1:41 AM Executable Jar File 10 KB
webservices 7/13/2012 1:41 AM Executable Jar File 143 KB

Tabla de SSIS PSFEED(ver tabla 54)

Tabla 54 – Tabla de SSIS PSFEED

NNo.	Input/Output	Nombre del conector	Tipo de conexiòn	Ruta destino
1	input	GU EMPID Upload	File	\\HQPAPROVN\psfeed$\input\GlobalUsers.csv
2	Input	psfeed input	File	\\itfectp07\dataprop\prov_file.txt

NNo.	Input/Output	Nombre del conector	Tipo de conexión	Ruta destino
1	Input/Output	CONN_IDBDBA	ODBC	Server: IDBpRDB2\IDBpRDB2INST2 Database: IDBDBA
2	Input/Output	Microsoft OLE DB Provider for SQL Server	ODBC	Server: idbprda1\idbprda1inst1 Database: ETAPSDBPRD

NNo.	Input/Output	Nombre del conector	Tipo de conexión	Ruta destino
1	Output	CONN_IADBPSFEED1_Log.txt	File	\\HQPAPROVN\psfeed$\CAIM_IADBPSFEED1_SSIS_log\CAIM_IADBPSFEED1_Log.txt
2	Output	Exisiting_Users	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\existing_users.csv
3	Output	Failsafe Error Message	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\failsafe_errormessage.csv
4	Output	GU Updated Non Staff	File	\\HQPAPROVN\psfeed$\output\NONSTAFF\GU_updates_nonstaff.csv

453

5	Output	New User Exception Duplicates	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\New_Users_Exception.csv
6	Output	new users role faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\new_users_role_faildump.csv
7	Output	New User Exception Duplicates	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\New_Users_Exception.csv
8	Output	new users role faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\new_users_role_faildump.csv
9	Output	New Users Role NON STAFF	File	\\HQPAPROVN\psfeed$\output\NONSTAFF\new_users_role_nonstaff.csv
10	Output	new users role nonstaff faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\new_users_role_nonstaff_faildump.csv
11	Output	new_users_role	File	\\HQPAPROVN\psfeed$\output\STAFF\new_users_role.csv
12	Output	rehire users role nonstaff faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\rehired_users_role_nonstaff_faildump.csv
13	Output	Rehired Users	File	\\HQPAPROVN\psfeed$\output\STAFF\rehired_users_role.csv
14	Output	rehired users role fail dump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\rehired_users_role_faildump.csv
15	Output	Rehired Users Role NON STAFF	File	\\HQPAPROVN\psfeed$\output\NONSTAFF\rehired_users_role_nonstaff.csv
16	Output	Role_Dept_Missing	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\Role_Dept_Missing_Exception.csv
17	Output	Terminated Users	File	\\HQPAPROVN\psfeed$\output\STAFF\terminated_users.csv

454

18	Output	terminated users faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\terminated_users_faildump.csv
19	Output	Terminated users Non STAFF	File	\\HQPAPROVN\psfeed$\output\NONSTAFF\terminated_users_nonstaff.csv
20	Output	Terminated users nonstaff faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\terminated_users_nonstaff_faildump.csv
21	Output	Text File (Destination)	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\New_Users_Exception.csv
22	Output	Transfer User Role	File	\\HQPAPROVN\psfeed$\output\STAFF\transferred_users_role.csv
23	Output	Transferred user role nonstaff faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\transferred_users_role_nonstaff_faildump.csv
24	Output	Transferred Users Role Faildump	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\transferred_users_role_faildump.csv
25	Output	Transferred users Role NON STAFF	File	\\HQPAPROVN\psfeed$\output\NONSTAFF\transferred_users_role_nonstaff.csv
26	Output	Updated Managers	File	\\HQPAPROVN\psfeed$\output\STAFF\updated_managers.csv
27	Output	User Name Exception	File	\\HQPAPROVN\psfeed$\output\EXCEPTIONS\username_exception.csv

455

Resultados y/o conclusiones.

Con la Implementación del sistema Enterprise Identity, Access Management(EIAM), Identity Manager(IDM) y Provisioning Manager(PM) en el Banco Interamericano de desarrollo se obtuvieron los siguientes beneficios:

Integración con el sistema de Recursos Humanos-ERP, de esta manera los accesos a los sistemas se crearán y otorgarán de acuerdo a la vigencia del contrato del usuario.(SAP, People Soft)

La configuración y conexion con las aplicaciones Active Directory, Oracle, Unix y Exchange fue exitosa, el sistema EIAM puede administrar de forma centralizada las aplicaciones y los usuarios que existan en ellas.

El sistema tiene el alcance de dar privilegios y accesos a los usuarios, bloquear y reactivar ceuntas, remover accesos, hacer cambios de contraseña, mover cuentas de un contenedor a otro, encontrar cuentas huerfanas y localizar al dueño de la cuenta.

El sistema es capaz de generar reportes historicos de los eventos de provisionamiento

456

Referencias Bibliograficas.

1. La fábrica de software moderna – CA Technologies 2017, www.ca.com/es

2. Sailpoint University 2017, www.sailpoint.com

3. CISA Certified Information Systems Auditor. 2017

- CA Identity Manager – CA Technologies, Nov 11, 2017, www.ca.com/us/products/ca-identity-manager.html

4. SailPoint - Identity Governance & Cloud Identity Management, 2017, www.sailpoint.com

- Daltabuit, Enrique. 2007. La seguridad de la información. Limusa, México.

- Wylder, John. 2004. Strategic Information Security. AUERBACH

- Tudor, Jan Killmeyer. 2001. Information Security architecture: an integrated approach to security in the organization. AUERBACH

- Senn, James A. 1992. Análisis y Diseño de Sistemas de Información, Segunda edición.

- eTrust Access Control. For the Unix Administrator. ET100 Student Guide. CA Computer Associates. 2002 Computer Associates International, Inc.

- eTrust Audit. ET430 Student Guide. CA Computer Associates. 2004 Computer Associates International, Inc.

457

- CA Identity Minder Administration Guide 12.6.5

- Pino Caballero, Gil. Seguridad Informática Técnicas criptográficas. RA-MA

- Sanjurjo, C. L. 2004. Tecnologías de la Información. España: Ideas Propias.

- Laudon, K. 2004. Sistemas de Información Gerencial. México: Pearson Educación.

- King, P. H. 1988. Sistemas Expertos. España: Díaz de Santos.

- People Soft, 2015, www.oracle.com

- SAP, 2017, www.SAP.com

458