



# Notas de la versión de Sun Java System Access Manager 7.1 para Microsoft Windows



Sun Microsystems, Inc.  
4150 Network Circle  
Santa Clara, CA 95054  
U.S.A.

Referencia: 820-1793-10  
Febrero de 2007

Copyright 2007 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Reservados todos los derechos.

Sun Microsystems, Inc. tiene los derechos de propiedad intelectual relacionados con la tecnología incluida en este producto. En concreto, y sin limitarse a ello, estos derechos de propiedad intelectual pueden incluir una o más patentes de EE.UU. o aplicaciones pendientes de patente en EE.UU. y otros países.

Derechos del gobierno de los EE. UU. – Software comercial. Los usuarios gubernamentales están sujetos al acuerdo de licencia estándar de Sun Microsystems, Inc. y a las disposiciones aplicables de la regulación FAR y sus suplementos.

Esta distribución puede incluir componentes desarrollados por terceros.

Determinadas partes del producto pueden derivarse de Berkeley BSD Systems, con licencia de la Universidad de California. UNIX es una marca registrada en los EE.UU. y otros países, bajo licencia exclusiva de X/Open Company, Ltd.

Sun, Sun Microsystems, el logotipo de Sun, el logotipo de Solaris, el logotipo de la taza de café de Java, docs.sun.com, Java y Solaris son marcas comerciales o marcas comerciales registradas de Sun Microsystems, Inc. en EE.UU. y otros países. Todas las marcas comerciales SPARC se usan bajo licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. en los EE.UU. y en otros países. Los productos que lleven marcas comerciales SPARC se basan en una arquitectura desarrollada por Sun Microsystems, Inc.

La interfaz gráfica de usuario OPEN LOOK y Sun<sup>TM</sup> fue desarrollada por Sun Microsystems, Inc. para sus usuarios y licenciatarios. Sun reconoce los esfuerzos pioneros de Xerox en la investigación y el desarrollo del concepto de interfaces gráficas o visuales de usuario para el sector informático. Sun dispone de una licencia no exclusiva de Xerox para la interfaz gráfica de usuario de Xerox, que es extensiva a los licenciatarios de Sun que implementen la interfaz gráfica de usuario OPEN LOOK y que actúen conforme a los acuerdos de licencia por escrito de Sun.

Los productos que se tratan y la información contenida en esta publicación están controlados por las leyes de control de exportación de los Estados Unidos y pueden estar sujetos a leyes de exportación o importación en otros países. Queda terminantemente prohibido el uso final (directo o indirecto) de esta documentación para el desarrollo de armas nucleares, químicas, biológicas, de uso marítimo nuclear o misiles. Queda terminantemente prohibida la exportación o reexportación a países sujetos al embargo de los Estados Unidos o a entidades identificadas en las listas de exclusión de exportación de los Estados Unidos, incluidas, pero no de forma excluyente, las personas con acceso denegado y las listas de ciudadanos designados especialmente.

ESTA DOCUMENTACIÓN SE PROPORCIONA "TAL CUAL". SE RECHAZAN TODAS LAS CONDICIONES, REPRESENTACIONES Y GARANTÍAS, EXPRESAS O IMPLÍCITAS, INCLUIDAS CUALQUIER GARANTÍA IMPLÍCITA DE COMERCIALIZACIÓN, ADECUACIÓN PARA UNA FINALIDAD DETERMINADA O DE NO CONTRAVENCIÓN, EXCEPTO EN AQUELLOS CASOS EN QUE DICHA RENUNCIA NO FUERA LEGALMENTE VÁLIDA.

# Contenido

---

<b>1</b>	<b>Notas de la versión de Sun Java System Access Manager 7.1 para Microsoft Windows</b>	<b>5</b>
	Acerca de Sun Java System Access Manager 7.1	5
	Novedades de esta versión	6
	Integración de la estructura de supervisión de Java ES	6
	Seguridad del Servicio web	7
	Implementación de un único archivo WAR de Access Manager	7
	Mejoras de los servicios principales	7
	Requisitos de hardware y software	10
	Exploradores compatibles	11
	Información general de compatibilidad	12
	Modo tradicional de Access Manager	12
	Agentes de directivas de Access Manager	13
	Otros problemas conocidos y limitaciones	13
	Problemas de instalación	13
	Problemas de actualización	14
	Problemas de configuración	15
	Problemas de la consola de Access Manager	16
	Problemas de SDK y de cliente	17
	Problemas de sesión y SSO	18
	Problemas de directivas	18
	Problemas de inicio del servidor	18
	Problemas de federación y SAML	19
	Problemas de internacionalización (g11n)	19
	Problemas de documentación	21
	Actualizaciones de la documentación	22
	Archivos que se pueden distribuir	22
	Información sobre problemas y respuestas de los clientes	23
	Sun valora sus comentarios	23

Recursos adicionales de Sun .....	23
Funciones de accesibilidad para discapacitados .....	24
Sitios web de terceros relacionados .....	24

# Notas de la versión de Sun Java System Access Manager 7.1 para Microsoft Windows

---

Las Notas de la versión de Sun Java™ System Access Manager 7.1 contienen información importante disponible para esta versión de Sun Java Enterprise System (Java ES), incluidas las nuevas funciones de Access Manager y problemas conocidos junto con sus soluciones, si hay alguna disponible. Lea este documento antes de instalar y utilizar esta versión.

Para consultar la documentación del producto Java ES, incluida la recopilación sobre Access Manager, consulte <http://docs.sun.com/prod/entsys.05q4>. Visite este sitio antes de instalar y configurar el software y, después, de forma periódica para consultar la documentación más reciente.

Las Notas de la versión de Access Manager 7.1 contienen las siguientes secciones:

- “Acerca de Sun Java System Access Manager 7.1” en la página 5
- “Novedades de esta versión” en la página 6
- “Requisitos de hardware y software” en la página 10
- “Información general de compatibilidad” en la página 12
- “Otros problemas conocidos y limitaciones” en la página 13
- “Actualizaciones de la documentación” en la página 22
- “Archivos que se pueden distribuir” en la página 22
- “Información sobre problemas y respuestas de los clientes” en la página 23
- “Recursos adicionales de Sun” en la página 23
- “Sitios web de terceros relacionados” en la página 24

## Acerca de Sun Java System Access Manager 7.1

Sun Java System Access Manager forma parte de la infraestructura de Sun Identity Management que permite a una organización administrar el acceso seguro a aplicaciones web y a otros recursos de una empresa y entre cadenas de valores de empresa a empresa (business-to-business, B2B). Access Manager proporciona las siguientes funciones principales:

- Servicios de autenticación y autorización centralizados mediante un control de acceso basado en roles y reglas

- Inicio de sesión único (Single sign-on, SSO) para el acceso a las aplicaciones basadas en web de las organizaciones
- Compatibilidad de identidad federada con Liberty Alliance Project y el Lenguaje de marcas de aserción de seguridad (Security Assertions Markup Language, SAML)
- Registro de la información vital, incluidas las actividades de los usuarios y el administrador por parte de los componentes de Access Manager para las consiguientes operaciones de análisis, elaboración de informes y auditoría.

## Novedades de esta versión

Esta versión incluye las siguientes funciones nuevas:

- “Integración de la estructura de supervisión de Java ES” en la página 6
- “Seguridad del Servicio web” en la página 7
- “Implementación de un único archivo WAR de Access Manager ” en la página 7
- “Mejoras de los servicios principales” en la página 7

## Integración de la estructura de supervisión de Java ES

Access Manager 7.1 se integra en la estructura de supervisión de Java Enterprise System mediante extensiones de administración de Java (JMX). La tecnología JMX proporciona las herramientas para crear soluciones dinámicas, modulares y basadas en web para administrar y supervisar los dispositivos, las aplicaciones y las redes controladas por el servicio. Entre los usos típicos de la tecnología JMX se incluyen la consulta y el cambio de configuración de aplicaciones, la acumulación de estadísticas sobre comportamiento de aplicaciones, y la notificación de cambios de estado y comportamientos erróneos. Los datos se entregan a una consola de supervisión centralizada.

Access Manager 7.1 utiliza la estructura de supervisión de Java ES para capturar datos relacionados con los servicios y las estadísticas, entre los que se incluyen:

- Número de intentos de autenticación, y autenticaciones realizadas con éxito y no satisfactorias
- Número de sesiones activas y estadísticas de la base de datos de conmutación por error de sesión
- Estadísticas de la base de datos de conmutación por error de sesión
- Estadísticas de almacenamiento en la caché de directivas
- Tiempos de transacción de evaluación de directivas
- Número de afirmaciones de un proveedor determinado en una implementación de SAML/Federation

## Seguridad del Servicio web

Access Manager 7.1 amplía las capacidades de autenticación de los servicios web de la siguiente manera:

- Inserta símbolos en los mensajes salientes
- Evalúa los mensajes entrantes en busca de símbolos de seguridad
- Habilita la selección mediante clics de los proveedores de autenticación para nuevas aplicaciones

## Implementación de un único archivo WAR de Access Manager

Access Manager incluye un único archivo WAR que puede utilizar para implementar los servicios de Access Manager de forma coherente en cualquiera de los contenedores compatibles incluidos en una de las plataformas admitidas. El archivo WAR de Access Manager coexiste con el programa de instalación de Java Enterprise System que implementa varios archivos JAR, XML, JSP, HTML, GIF y de propiedades.

## Mejoras de los servicios principales

### Contenedores web admitidos

- Sun Java System Web Server 7.0
- Sun Java System Application Server 8.2
- BEA WL 8.1 SP4
- IBM WebSphere 5.1.1.6

### Integración con la estructura de supervisión

Access Manager puede utilizar la estructura de supervisión de JES para supervisar lo siguiente:

- Autenticación
  - Número de intentos de autenticación
  - Número de intentos de autenticación remota (opcional)
  - Número de autenticaciones realizadas con éxito
  - Número de autenticaciones no satisfactorias
  - Número de operaciones de cierre de sesión realizadas con éxito
  - Número de operaciones de cierre de sesión erróneas (opcional)
  - Tiempo de transacción para cada módulo, si es posible, en estado de ejecución y de espera

- Fallos de conectividad para los servidores secundarios
- Sesiones
  - Tamaño de la tabla de sesiones, que indica el número máximo de sesiones
  - Número de sesiones activas utilizando un contador incremental
  - Conmutación por error de sesión, incluido el número de sesiones “almacenadas” o el recuento de sesiones utilizando un contador incremental y el número de operaciones realizadas en la base de datos de conmutación por error, incluida la lectura, la escritura, la eliminación y número de operaciones.
- Servicio de administración de usuarios/ depósito de identidades/ administración de sesiones
  - Tamaño máximo de caché
  - Estadísticas relacionadas con la caché como, por ejemplo, el número de visitas, frecuencia, pico, tamaño actual, etc.
  - Tiempo de transacción de las operaciones en ejecución y en espera
- Directiva
  - Número de directivas en la caché
  - Número de `policyManagers` en la caché
  - Número de nombres de servicio en la caché de `policyListener`
  - Número de servicios en `resultsCache`
  - Número de `tokenIDs` en `sessionListenerRegistry`
  - Número de nombres de servicio en `policyListenerRegistry`
  - Número de `tokenIDs` en la caché de `role`
  - Número de nombres de servicio en la caché de `resourceNames`
  - Número de entradas para `SubjectEvaluationCache`
  - Número de `PolicyEvaluators` en la caché
  - Número de escuchas de cambio de directiva en la caché
  - Tiempo de transacción para el procesamiento de evaluación de directivas
- Federación
  - Número de artefactos en la tabla para un proveedor determinado
  - Número de afirmaciones en la tabla para un proveedor determinado
  - Número de entradas de sesión en una tabla determinada para un Id. de proveedor determinado
- SAML
  - Tamaño del mapa de artefactos
  - Tamaño del mapa de afirmaciones

## Módulo de autenticación

- El servicio de autenticación distribuida no es necesario para utilizar un solo servidor para las implementaciones de carga equilibrada.
- El servidor y el servicio de autenticación no son necesarios para utilizar un solo servidor para las implementaciones de carga equilibrada.
- Compatibilidad con los consejos compuestos entre el servicio de autenticación, los agentes de directivas y el servicio de directivas. Esta compatibilidad incluye la condición `AuthenticateToRealm`, `AuthenticateToService` y la idoneidad del dominio para todas las condiciones.
- Organización de consejo mediante condiciones de autenticación calificadas para el dominio.
- Configuraciones de autenticación/cadenas de autenticación (`AuthServiceCondition`).
- Ahora la autenticación basada en módulos puede desactivarse si se aplica el encadenamiento de autenticación.
- El servicio de autenticación distribuida admite el módulo de autenticación de certificados.
- Se ha agregado `CertAuth` a la IU de autenticación distribuida para convertirla en una presentación de extractor de credenciales con todas las funciones.
- El nuevo módulo de autenticación de almacén de datos es un módulo comercializable que se autentica en el almacén de datos configurado de un dominio concreto.
- Ahora la configuración de bloqueo de cuenta se mantiene en varias instancias del servidor AM.
- Encadenamiento de clases SPI de procesamiento posterior.

## Módulo de directiva

- Compatibilidad con la definición de directivas en función de la autenticación basada en el servicio.
- Se ha agregado una nueva condición de directiva: `AuthenticateToRealmCondition`.
- Compatibilidad con la comparación de caracteres comodín de un nivel para facilitar la protección del contenido del directorio sin proteger el subdirectorio.
- Compatibilidad con la condición de filtro LDAP. La administración de directivas puede especificar un filtro LDAP en la condición a la vez que se define una directiva.
- Se pueden crear directivas en subdominios sin directivas de referencia explícitas desde el dominio principal si se ha habilitado una referencia al alias de la organización en la configuración global de directivas.
- `AuthLevelCondition` puede especificar el nombre del domino, además del nivel de autenticación.
- `AuthSchemeCondition` puede especificar el nombre del dominio, además del nombre del módulo de autenticación.

### Módulo de administración de servicios

- Compatibilidad con el almacenamiento de la configuración de administración de servicios/directivas en Active Directory.

### Access Manager SDK

- Compatibilidad de las API con la autenticación de usuarios en una base de datos de la estructura del depósito de identidades predeterminada.

### Compatibilidad con los servicios web

- Proveedor SOAP de Liberty ID-WSF: proveedor de autenticación que encapsula el enlace SOAP de Liberty ID-WSF del mismo modo que Access Manager lo implementa. Este proveedor consta de un cliente y un proveedor de servidor.
- Proveedor SSO de capa HTTP: proveedor de autenticación de capa `HttpServlet` que encapsula SSO de servidor basado en Access Manager.

### Módulo de instalación

- Vuelve a empaquetar Access Manager como una aplicación J2EE, lo que da lugar a un único archivo WAR que se puede implementar en la Web.

### Módulo de delegación

- Compatibilidad con la agrupación de los privilegios de delegación

### Registro

- Compatibilidad con la delegación en el módulo de registro, que controla las identidades autorizadas para escribir o leer en los archivos de registro.
- Compatibilidad con `SecureLogHelper` basado en JCE, lo que permite utilizar JCE, además de JSS, como un proveedor de seguridad para la implementación del registro seguro.

## Requisitos de hardware y software

La siguiente tabla muestra los requisitos de hardware y software para esta versión.

TABLA 1-1 Requisitos de hardware y software

Componente	Requisito
Sistema operativo (SO)	<ul style="list-style-type: none"> <li>▪ Windows 2000 Advance Server SP4</li> <li>▪ Windows XP SP2</li> <li>▪ Windows 2003 Enterprise Server SP1 (32 bits)</li> <li>▪ Windows 2003 Enterprise Server SP1 (64 bits)</li> </ul>

TABLA 1-1 Requisitos de hardware y software (Continuación)

Componente	Requisito
Java 2 Standard Edition (plataforma J2SE™)	Plataforma J2SE 6.0, 5.0 Actualización 7 y 1.4.2 Actualización 11
Directory Server	Árbol de información de Access Manager: Sun Java System Directory Server 5.2  Repositorio de identidades de Access Manager: Sun Java System Directory Server 6.0 o Microsoft Active Directory
Contenedores web	Sun Java System Web Server 7.0  Sun Java System Application Server Enterprise Edition 8.2
RAM	Prueba básica: 512 Mbytes  Implementación real: 1 Gbyte para los subprocesos, Access Manager SDK, el servidor HTTP y otros componentes internos
Espacio en disco	512 Mbytes para Access Manager y las aplicaciones asociadas

Si tiene alguna duda sobre la compatibilidad con otras versiones de estos componentes, póngase en contacto con el representante técnico de Sun Microsystems.

## Exploradores compatibles

La siguiente tabla muestra los exploradores compatibles con la versión Sun Java Enterprise System 5.

TABLA 1-2 Exploradores compatibles

Explorador	Plataforma
Firefox 1.0.7	Windows XP Windows 2000
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000
Mozilla 1.7.12	Windows XP Windows 2000

TABLA 1-2 Exploradores compatibles (Continuación)

Explorador	Plataforma
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000

## Información general de compatibilidad

- “Modo tradicional de Access Manager” en la página 12
- “Agentes de directivas de Access Manager” en la página 13

## Modo tradicional de Access Manager

Si instala Access Manager con Sun Java System Portal Server, debe seleccionar el modo tradicional (6.x) de Access Manager. Para determinar el modo de instalación de Access Manager 7.1, consulte [“Determinar el modo de Access Manager” en la página 12](#).

### Opción Configurar automáticamente durante la instalación

Si está ejecutando el programa de instalación de Java ES en modo gráfico con la opción Configurar automáticamente durante la instalación, Access Manager se configura en modo "tradicional (estilo de la versión 6.x)".

### Opción Configurar manualmente después de la instalación

Si ejecutó el programa de instalación de Java ES con la opción Configurar manualmente después de la instalación, debe ejecutar el archivo `install-dir\identity\setup\amconfig.bat` para configurar Access Manager después de la instalación. Para seleccionar el modo tradicional (6.x), establezca el siguiente parámetro en el archivo de configuración

```
AM_REALM = disabled
```

```
...
install-dir\identity\setup\AMConfigurator.properties
...
```

### Determinar el modo de Access Manager

Para determinar si la instalación de Access Manager 7.1 que se está ejecutando se ha configurado en el modo tradicional o de dominio, escriba:

```
http(s)://host:port/amserver/SMSServlet?method=isRealmEnabled
```

El valor de retorno `true` (verdadero) indica el modo de dominio. El valor de retorno `false` (falso) indica el modo tradicional.

## Agentes de directivas de Access Manager

La siguiente tabla muestra la compatibilidad de los agentes de directivas con los modos de Access Manager 7.1.

**TABLA 1-3** Compatibilidad de los agentes de directivas con los modos de Access Manager 7.1

Agente y versión	Modo compatible
Agentes web y J2EE, versión 2.2	Modos tradicional y de dominio
Agentes web, versión 2.1	Modos tradicional y de dominio
Agentes J2EE, versión 2.1	Sólo en modo tradicional

## Otros problemas conocidos y limitaciones

En esta sección, se describen los siguientes problemas conocidos y sus soluciones (si las hay) en el momento de la publicación de Access Manager 7.0.

- [“Problemas de instalación” en la página 13](#)
- [“Problemas de configuración” en la página 15](#)
- [“Problemas de la consola de Access Manager” en la página 16](#)
- [“Problemas de SDK y de cliente” en la página 17](#)
- [“Problemas de sesión y SSO” en la página 18](#)
- [“Problemas de directivas” en la página 18](#)
- [“Problemas de inicio del servidor” en la página 18](#)
- [“Problemas de federación y SAML” en la página 19](#)
- [“Problemas de internacionalización \(g11n\)” en la página 19](#)
- [“Problemas de documentación” en la página 21](#)

## Problemas de instalación

- [“Al instalar Access Manager en un árbol de información de directorio \(DIT\) existente, es necesario volver a generar los índices de Directory Server. \(6268096\)” en la página 14](#)
- [“El servicio de autenticación no se inicializa cuando Access Manager y Directory Server están instalados en equipos distintos. \(6229897\)” en la página 14](#)

## Al instalar Access Manager en un árbol de información de directorio (DIT) existente, es necesario volver a generar los índices de Directory Server. (6268096)

Para mejorar el rendimiento de las búsquedas, Directory Server dispone de varios nuevos índices.

**Solución:** una vez instalado Access Manager con un árbol de información de directorio (DIT), vuelva a generar los índices de Directory Server ejecutando la secuencia de comandos `db2index.pl`. Por ejemplo:

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

La secuencia de comandos `db2index.pl` se encuentra disponible en el directorio *DS-install-directory/slapd-hostname*.

## El servicio de autenticación no se inicializa cuando Access Manager y Directory Server están instalados en equipos distintos. (6229897)

Aunque `classpath` y otras variables de entorno del contenedor web de Access Manager se actualizan durante la instalación, el proceso de instalación no reinicia el contenedor web. Si intenta iniciar una sesión en Access Manager tras la instalación antes de reiniciar el contenedor web, se devuelve el siguiente error:

```
Authentication Service is not initialized.  
Contact your system administrator.
```

**Solución:** reinicie el contenedor web antes de iniciar una sesión en Access Manager. Directory Server también debe ejecutarse antes de iniciar una sesión.

## Problemas de actualización

- “Portal Server y Web Console no funcionan tras actualizar Access Manager de Java ES 4 a Java ES 5. (6515054)” en la página 14

### Portal Server y Web Console no funcionan tras actualizar Access Manager de Java ES 4 a Java ES 5. (6515054)

Tras actualizar Access Manager de Java ES 4 a Java ES 5, las aplicaciones implementadas, Portal Server y Web Console no funcionan.

**Solución:** copie el archivo `config.properties` de la ubicación de la instalación de Java ES 5 a la ubicación de la instalación de Java ES 4:

```
copy install-Dir\share\MobileAccess\config\config.properties  
JavaES4-install-dir\PortalServer\https-host-name\portal\web-apps\WEB-INF\classes\
```

## Problemas de configuración

- “Se requiere Active Perl 5.8 o superior para configurar algunos módulos de Access Manager.” en la página 15
- “El programa de instalación no puede configurar los componentes de autenticación distribuida y SDK de cliente.” en la página 15
- “ Los archivos am2bak.bat y bak2am.bat no se generan correctamente. (6491091)” en la página 15
- “La cuenta de usuario no se desactiva tras muchos sucesivos inicios de sesión insatisfactorios. (6469200)” en la página 15

### Se requiere Active Perl 5.8 o superior para configurar algunos módulos de Access Manager.

Es necesario instalar Active Perl 5.8 o superior para configurar los siguientes componentes con Access Manager:

- MFWK
- Conmutación por error de sesión
- Federación masiva
- Ajuste del rendimiento

Puede descargar Active Perl desde <http://www.activestate.com/Products/ActivePerl/>.

### El programa de instalación no puede configurar los componentes de autenticación distribuida y SDK de cliente.

En Configurar automáticamente durante la instalación, los componentes de autenticación distribuida y SDK de cliente no se configuran. No se muestra ningún mensaje de error.

**Solución:** utilice la opción Configurar manualmente después de la instalación durante la instalación y configure manualmente los componentes de autenticación distribuida y SDK de cliente después de la instalación.

### Los archivos am2bak.bat y bak2am.bat no se generan correctamente. (6491091)

Access Manager 7.1 no es compatible con las utilidades de copia de seguridad (am2bak.bat) y restauración (bak2am.bat).

**Solución:** ninguna.

### La cuenta de usuario no se desactiva tras muchos sucesivos inicios de sesión insatisfactorios. (6469200)

La cuenta de usuario no se desactiva tras varios inicios de sesión insatisfactorios en Access Manager.

**Solución:** Utilice la consola de administración de dominio (`\amserver\console`) para habilitar o deshabilitar la utilidad de bloqueo. Para establecer el atributo Modo de bloqueo de error de inicio de sesión, siga estos pasos:

1. Abra la GUI de Access Manager.
2. Seleccione un dominio para habilitar el bloqueo.
3. Seleccione la ficha Autenticación.
4. Haga clic en el botón Propiedades avanzadas.
5. Seleccione el atributo Modo de bloqueo de error de inicio de sesión.
6. Guarde las propiedades haciendo clic en el botón Guardar.

## Problemas de la consola de Access Manager

- “La nueva consola de Access Manager no puede establecer las prioridades de plantilla de CoS. (6309262)” en la página 16
- “Aparece la antigua consola al agregar servicios relacionados con Portal Server. (6293299)” en la página 16
- “La consola no devuelve el conjunto de resultados de Directory Server una vez alcanzado el límite de recursos. (6239724)” en la página 17

### La nueva consola de Access Manager no puede establecer las prioridades de plantilla de CoS. (6309262)

La nueva consola de Access Manager 7.1 no puede establecer ni modificar una prioridad de plantilla de Clase de servicio (CoS).

**Solución:** inicie una sesión en la consola de Access Manager 6 2005Q1 para establecer o modificar la prioridad de plantilla de CoS.

### Aparece la antigua consola al agregar servicios relacionados con Portal Server. (6293299)

Portal Server y Access Manager se instalan en el mismo servidor. Con Access Manager instalado en el modo tradicional, inicie una sesión en la nueva consola mediante `/amserver`. Si se selecciona un usuario existente y se intentan agregar servicios como NetFile o Netlet, aparecerá la antigua consola de Access Manager (`/amconsole`).

**Solución:** ninguna. La versión actual de Portal Server requiere la consola de Access Manager 6 2005Q1.

## La consola no devuelve el conjunto de resultados de Directory Server una vez alcanzado el límite de recursos. (6239724)

En la siguiente situación, la consola no muestra información precisa: instale Directory Server y, a continuación, Access Manager con la opción de DIT existente. Inicie una sesión en la consola de Access Manager y cree un grupo. Edite los usuarios del grupo, por ejemplo, añada usuarios con el filtro `uid=*999*`. La lista resultante estará vacía y la consola no mostrará ningún mensaje de error, advertencia o informativo.

**Solución:** los miembros del grupo no deben superar el límite de tamaño de búsqueda de Directory Server. En caso contrario, cambie el límite de tamaño de búsqueda proporcionalmente.

## Problemas de SDK y de cliente

- “No se puede crear el mismo usuario eliminado a través del portal. (6479611)” en la página 17
- “Los clientes no reciben notificaciones después de reiniciarse el servidor. (6309161)” en la página 17
- “Los clientes SDK deben reiniciarse después del cambio de esquema de servicio. (6292616)” en la página 17

### No se puede crear el mismo usuario eliminado a través del portal. (6479611)

No puede crear el mismo perfil de usuario eliminado a través del portal. Aparecerá el siguiente mensaje de error:

```
An error occurred while storing the user profile.
```

**Solución:** ninguna.

### Los clientes no reciben notificaciones después de reiniciarse el servidor. (6309161)

Las aplicaciones escritas con el cliente SDK (`amclientsdk.jar`) no reciben notificaciones si se reinicia el servidor.

**Solución:** ninguna.

### Los clientes SDK deben reiniciarse después del cambio de esquema de servicio. (6292616)

Si se modifica un esquema de servicio, `ServiceSchema.getGlobalSchema` devuelve el antiguo esquema en lugar del nuevo.

**Solución:** reinicie el cliente tras modificar un esquema de servicio.

## Problemas de sesión y SSO

### Utilización de HttpSession con contenedores web de terceros

El método predeterminado para mantener las sesiones de autenticación es “sesión interna” en lugar de HttpSession. El valor predeterminado de tiempo máximo de sesión no válida de tres minutos es suficiente. La secuencia de comandos `amtune` define este valor en un minuto para Web Server o Application Server. Sin embargo, si utiliza un contenedor web de terceros como, por ejemplo, IBM WebSphere o el servidor BEA WebLogic y el elemento opcional `HttpSession`, es posible que necesite limitar el tiempo máximo de HttpSession del contenedor web para evitar problemas de rendimiento.

## Problemas de directivas

### La eliminación de atributos dinámicos en el servicio de configuración de directivas provoca problemas de edición de directivas. (6299074)

La eliminación de atributos dinámicos en el servicio de configuración de directivas provoca problemas al editar las directivas, como se muestra a continuación:

1. Cree dos atributos dinámicos en el servicio de configuración de directivas.
2. Cree una directiva y seleccione los atributos dinámicos recientemente creados en el proveedor de respuestas.
3. Elimine los atributos dinámicos en el servicio de configuración de directivas y cree dos atributos adicionales.
4. Intente editar la directiva creada en el paso 2.

Aparecerá el siguiente mensaje de error: "Error, se está estableciendo una propiedad dinámica no válida" (Error Invalid Dynamic property being set). No se muestra de forma predeterminada ninguna directiva en la lista. Después de realizar la búsqueda, se mostrarán las directivas, pero no se podrán editar o eliminar las directivas existentes ni crear una nueva.

**Solución:** antes de eliminar los atributos dinámicos del servicio de configuración de directivas, elimine las referencias a dichos atributos en las directivas.

## Problemas de inicio del servidor

### Error de depuración al iniciar Access Manager. (6309274, 6308646)

Al iniciar Access Manager 7.1, se devuelven los siguientes errores de depuración en los archivos `amDelegation` y `amProfile`:

- `amDelegation`: no se puede obtener una instancia del complemento para la delegación.

- `amProfile`: se recibió una excepción de delegación.

**Solución:** ninguna. No tenga en cuenta estos mensajes.

## Problemas de federación y SAML

- “La federación presenta errores al utilizar el perfil de artefacto. (6324056)” en la página 19
- “Error de cierre de sesión en la federación. (6291744)” en la página 19

### La federación presenta errores al utilizar el perfil de artefacto. (6324056)

Si se configuran un proveedor de identidades (IDP, Identity Provider) y un proveedor de servicios (SP, Service Provider), se cambia el protocolo de comunicación para utilizar el perfil de artefacto del explorador y, a continuación, se intenta realizar la federación de usuarios entre el IDP y el SP, el proceso de federación fallará.

**Solución:** ninguna.

### Error de cierre de sesión en la federación. (6291744)

En el modo de dominio, si se intenta realizar la federación de cuentas de usuario en un proveedor de identidades (IDP) y un proveedor de servicios (SP), se finaliza la federación y, a continuación, se cierra la sesión; se mostrará el siguiente mensaje de error: Error: no se ha encontrado ninguna suborganización (Error: No sub organization found.)

**Solución:** ninguna.

## Problemas de internacionalización (g11n)

- “Aparece un error de aplicación en el panel izquierdo de la Ayuda en línea de la consola de dominio. (6508103)” en la página 19
- “No se puede eliminar UTF-8 en la sección de detección de cliente. (5028779)” en la página 20
- “Los caracteres multibyte se muestran en forma de signos de interrogación en los archivos de registro. (5014120)” en la página 20

### Aparece un error de aplicación en el panel izquierdo de la Ayuda en línea de la consola de dominio. (6508103)

Si se implementa Access Manager en Application Server, el panel izquierdo de la Ayuda en línea de la consola de dominio muestra un error de aplicación.

**Solución:** siga estos pasos:

1. Copie el archivo `jhall.jar`.  
`copy install-dir\share\lib\jhall.jar %JAVA_HOME%\jre\lib\ext`
2. Reinicie Application Server.

## **No se puede eliminar UTF-8 en la sección de detección de cliente. (5028779)**

La función de detección de cliente no funciona correctamente. Los cambios realizados en la consola de Access Manager 7.1 no se transfieren automáticamente al explorador.

**Solución:**pruebe con las siguientes soluciones:

1. Reinicie el contenedor web de Access Manager después de realizar un cambio en la sección de detección de cliente.
2. Realice los siguientes pasos en la consola de Access Manager:
  - a. Haga clic en **Client Detection** en la ficha **Configuration**.
  - b. Haga clic en el vínculo **Edit** para **genericHTML**.
  - c. En la ficha **HTML**, haga clic en el vínculo **genericHTML**.
  - d. Introduzca la siguiente entrada en la lista de juegos de caracteres: **UTF-8;q=0.5** (Asegúrese de que el factor **q** de UTF-8 sea inferior al de otros juegos de caracteres de su configuración regional.)
  - e. Haga clic en **Guardar**.
  - f. Cierre la sesión e inicie una sesión de nuevo.

## **Los caracteres multibyte se muestran en forma de signos de interrogación en los archivos de registro. (5014120)**

Los mensajes multibyte de los archivos de registro del directorio `install_dir\identity\logs` se muestran en forma de signos de interrogación (?). Los archivos de registro suelen presentar una codificación nativa y, no siempre, UTF-8. Cuando una instancia del contenedor web se inicia con una determinada configuración regional, los archivos de registro presentarán una codificación nativa para dicha configuración regional. Si se cambia a otra configuración regional y se reinicia la instancia del contenedor web, los mensajes actuales presentarán la codificación nativa para dicha configuración regional, pero los mensajes de codificaciones anteriores se mostrarán en forma de signos de interrogación.

**Solución:** asegúrese de iniciar siempre las instancias del contenedor web con la misma codificación nativa.

## Problemas de documentación

- “Información sobre la compatibilidad de los roles y los roles filtrados con el complemento LDAPv3. (6365196)” en la página 21
- “Información sobre las propiedades no utilizadas en el archivo `AMConfig.properties`. (6344530)” en la página 21
- “Información sobre cómo habilitar el cifrado XML. (6275563)” en la página 21

### Información sobre la compatibilidad de los roles y los roles filtrados con el complemento LDAPv3. (6365196)

Después de aplicar el respectivo parche, puede configurar los roles y los roles filtrados del complemento LDAPv3, si los datos se han almacenado en Sun Java System Directory Server. En , para

1. Acceda a la consola de administrador de Access Manager 7.1
2. Seleccione la configuración LDAPv3.
3. En el campo “Complemento LDAPv3 compatible con tipos y operaciones”, escriba los siguientes valores en función de los roles y los roles filtrados que desee utilizar en su configuración LDAPv3:

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

### Información sobre las propiedades no utilizadas en el archivo `AMConfig.properties`. (6344530)

Las siguientes propiedades del archivo `AMConfig.properties` no se utilizan:

```
com.ipplanet.am.directory.host
com.ipplanet.am.directory.port
```

### Información sobre cómo habilitar el cifrado XML. (6275563)

Para habilitar el cifrado XML, realice los siguientes pasos:

1. (Opcional) Si está utilizando una versión de JDK anterior a la versión 1.5.;
  - a. Descargue el proveedor JCE de Bouncy Castle desde el sitio de Bouncy Castle (<http://www.bouncycastle.org/>).  
Por ejemplo, para JDK 1.4, descargue el archivo `bcprov-jdk14-131.jar`.
  - b. Copie el archivo en el directorio `jdk_root\jre\lib\ext`.
2. Descargue los archivos de la directiva Unlimited Strength Jurisdiction de JCE para su versión de JDK.

- Para Sun Systems, descargue los archivos desde el sitio de Sun (<http://java.sun.com>) para su versión de JDK.
  - Para IBM WebSphere, acceda al sitio correspondiente de IBM para descargar los archivos necesarios.
3. Copie los archivos descargados `US_export_policy.jar` y `local_policy.jar` en el directorio `jdk_root/jre/lib/security`.
  4. Si utiliza una versión de JDK anterior a JDK 1.5, edite el archivo `jdk_root/jre/lib/security/java.security` y agregue Bouncy Castle como uno de los proveedores. Por ejemplo:  
  

```
security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
```
  5. Establezca la siguiente propiedad en el archivo `AMConfig.properties` como "true" (verdadera):  
  

```
com.sun.identity.jss.donotInstallAtHighestPriority=true
```
  6. Reinicie el contenedor web de Access Manager.

Para obtener más información, consulte el Id. de problema 5110285 (El cifrado XML requiere el archivo JAR de Bouncy Castle).

## Actualizaciones de la documentación

Estos documentos se encuentran disponibles en la colección de Access Manager 7.1 en <http://docs.sun.com/coll/1292.1>

La colección de Sun Java System Access Manager Policy Agent 2.2 también se ha revisado para documentar nuevos agentes y se encuentra disponible en <http://docs.sun.com/coll/1322.1>

## Archivos que se pueden distribuir

Sun Java System Access Manager 7.1 no contiene ningún archivo que se pueda distribuir a usuarios sin licencia de este producto.

## Información sobre problemas y respuestas de los clientes

Si experimenta problemas con Access Manager o Sun Java Enterprise System, póngase en contacto con el servicio de asistencia técnica de Sun usando uno de estos procedimientos:

- Servicios de recursos de asistencia técnica de Sun (SunSolve) en <http://sunsolve.sun.com/>.

Este sitio dispone de vínculos a la base de datos de soluciones, al centro de asistencia en línea y al rastreador de productos, así como a programas de mantenimiento y números de contacto de asistencia técnica.

- El número de teléfono del distribuidor asociado al contrato de mantenimiento

Para que podamos ayudarle de forma óptima en la solución de problemas, tenga a mano la siguiente información cuando se ponga en contacto con el servicio de asistencia técnica:

- Descripción del problema, incluida la situación en la que éste se produce y la forma en que afecta al funcionamiento
- Tipo de equipo, versión del sistema operativo y versión del producto, incluido cualquier parche del producto y otro software que pudiera influir en el problema
- Pasos detallados de los métodos que haya usado para solucionar el problema
- Cualquier registro de error o volcado del núcleo

## Sun valora sus comentarios

Sun tiene interés en mejorar su documentación, y agradece sus comentarios y sugerencias. Vaya a <http://docs.sun.com/> y haga clic en Send Comments (Enviar comentarios).

Indíquenos el título completo de la documentación y el número de referencia en los campos pertinentes. El número de referencia consta de siete o de nueve dígitos y se encuentra en la página que contiene el título de la guía o al principio del documento. Por ejemplo, el número de referencia de las *Access Manager Notas de la versión* es 819-5686.

## Recursos adicionales de Sun

Puede encontrar información útil y recursos de Access Manager en las siguientes direcciones de Internet:

- Documentación de Sun Java Enterprise System: <http://docs.sun.com/prod/entsys.05q4>
- Servicios de Sun: <http://www.sun.com/service/consulting/>
- Servicios y productos de software: <http://www.sun.com/software/>
- Recursos de asistencia técnica: <http://sunsolve.sun.com/>
- Información para programadores: <http://developers.sun.com/>

- Servicios de asistencia para programadores de Sun:  
<http://www.sun.com/developers/support/>

## Funciones de accesibilidad para discapacitados

Si desea disfrutar de las funciones de accesibilidad que se han comercializado tras la publicación de este soporte, consulte las valoraciones de productos de la Sección 508, que se pueden obtener de Sun previa solicitud, para determinar las versiones más adecuadas para implementar soluciones accesibles. Puede encontrar versiones actualizadas de las aplicaciones en <http://sun.com/software/javaenterprisesystem/get.html>.

Para obtener información sobre el compromiso de Sun con respecto a la accesibilidad, visite <http://sun.com/access>.

## Sitios web de terceros relacionados

En este documento se mencionan direcciones URL de terceros que proporcionan información adicional relacionada.

---

**Nota** – Sun no se responsabiliza de la disponibilidad de sitios web de terceros mencionados en este documento. Sun no garantiza ni se hace responsable de los contenidos, la publicidad, los productos u otros materiales que puedan estar disponibles a través de dichos sitios o recursos. Sun tampoco se hace responsable de ninguna pérdida o daño, real o supuesto, que se derive del uso de los contenidos, bienes o servicios que estén disponibles a través de estos sitios o recursos (o que pueda estar relacionado con ellos).

---