

Guía de Cambios

Última Versión
n10

© LEVER IT CORP.

Versión de Documento: 1.1

Copyright © 2014 Lever IT Corp. Todos los derechos reservados.

Los logos de Lever IT Corp., Discovery y Discovery Service Desk son marcas o marcas registradas de Lever IT Corp. O sus distribuidores principales en otros países.

Windows es una marca comercial de Microsoft Corporation. Otros nombres pueden ser marcas comerciales de sus respectivos propietarios.

El producto descrito en este documento se distribuye con licencias que limitan el uso, la copia, la distribución y la ingeniería inversa o descompilación.

LA DOCUMENTACIÓN SE PROPORCIONA "TALCUAL", Y SE RENUNCIA A TODAS LAS CONDICIONES IMPLÍCITAS O EXPRESAS, REPRESENTACIONES Y GARANTÍAS, INCLUIDA CUALQUIER GARANTÍA DE COMERCIABILIDAD, IDONEIDAD PARA UN FIN DETERMINADO O NO VIOLACIÓN DE DERECHOS, EXCEPTO EN CASO DE QUE LAS LIMITACIONES SE DECLAREN NO VÁLIDAS LEGALMENTE. LEVER IT CORP. NO SERÁ RESPONSABLE DE NINGÚN DAÑO INCIDENTAL O CONSECUENTE RELACIONADO CON LA ENTREGA, EL RENDIMIENTO O EL USO DE ESTA DOCUMENTACIÓN.

LA INFORMACIÓN QUE ESTE DOCUMENTO CONTIENE ESTÁ SUJETA A MODIFICACIONES SIN PREVIO AVISO.

Lever IT Corp.
www.leverit.com

Consola Web

Versión web a la consola de administración Discovery:

Funciones disponibles en la consola web: Versión 6.5.8.1

- Administrador de Información (Consultas, editables, gráficos).
- Consulta pestaña BDatos.
- Service Desk (Administrador de información, atención de reportes y traspaso de reportes, incluyendo sus herramientas de atención).
*No se incluyen funciones de administración y/o gestión de Service Desk.
*No se incluyen las funciones de Administración de Problemas.
- Características de Service Desk para **Grupos de Administradores(Perfiles)**, aplican según la siguiente tabla:

OPCIÓN DE PERFIL	FUNCIÓN	EN CONSOLA WEB
ADMINISTRACIÓN	Habilita/deshabilita: Asigna agente a administradores Administración de SLA Tiempo de Atención (Administración de horarios y calendarios)	NO APLICA En la Consola Web versión 6.5.7.4 las funciones administrativas de Service Desk no están disponibles
PAUSAR TICKET	Habilita/Deshabilita el botón Pausa en el panel de herramientas de Atención de Reportes	APLICA
CAMBIAR DE NIVEL	Habilita/Deshabilita el botón Escalar nivel al atender reporte ²¹	APLICA
PERMITE TRASPASOS DE OTROS TICKET	Habilita/Deshabilita la carpeta Asignación de Reportes (No Asignados, Traspaso de Reportes)	APLICA Nota: Se visualiza la vista Traspaso de Reportes. En la Consola Web versión 6.5.7.4 no se encuentra disponible la vista <i>No Asignados</i>
TRASPASOS EN ATENDER REPORTE	Habilita/Deshabilita el botón Transferir Reporte al atender reporte	APLICA
EDITAR CALIFICACIONES	Habilita/Deshabilita la vista Editar Calificaciones	NO APLICA En la Consola Web versión 6.5.7.4 la vista para calificación de reportes no está disponible
HERRAMIENTA ARCHIVOS ADJUNTOS	Habilita el botón Ejecuta Archivo S.D. en el panel de Ayuda Remota > Otras opciones	NO APLICA En la Consola Web versión 6.5.7.4 Las herramientas de Ayuda Remota no están habilitadas
EDITAR BASE DE CONOCIMIENTO	Habilita/Deshabilita la vista Configurar Conocimiento	NO APLICA En la Consola Web versión 6.5.7.4 las funciones administrativas de Service Desk no están habilitadas

VER TODOS LOS TEMAS	Al activar esta casilla se activa la restricción de <i>Temas por grupo</i> Cuando se deshabilita permite ver la totalidad de los temas, tanto para consulta de Base de conocimiento como para creación de nuevos temas y conocimientos. Nota: La restricción de Tema por grupo no aplica para la función Configurar Conocimiento	NO APLICA En la Consola Web versión 6.5.7.4 no se encuentra disponible esta función
CALIFICAR REPORTE	Habilita/Deshabilita el botón Calificar Reporte del panel de herramientas de Atención de Reportes	NO APLICA En la Consola Web versión 6.5.7.4 no se encuentra disponible esta función
CAMBIAR TEMA	Habilita/Deshabilita el botón Cambiar Tema al atender el reporte	APLICA
CAMBIAR URGENCIA	Habilita/Deshabilita el botón Cambiar Urgencia al Atender Reporte	APLICA
NUEVO REPORTE	Habilita/Deshabilita el botón Nuevo Reporte en la vista atención de reportes	APLICA

- Visualización de pestaña Extra y/o personalizaciones de vista realizadas en los SQL correspondientes a las vistas de Atención de Reportes y Traspaso de Reportes. No se incluyen vistas (públicas y privadas) creadas desde la *consola de administración > Atención de Reportes > Personaliza Rejilla*.

Complejidad de contraseñas

*Con la actualización a la versión 6.5.8.1

Si el usuario no ha cambiado contraseña va a solicitar cambio en el primer ingreso, la contraseña debe cumplir con las siguientes condiciones:

- La contraseña debe ser de mínimo 8 caracteres. El sistema recordará 10 últimas utilizadas para evitar que se repita.

- Debe incluir como mínimo 3 de los siguientes criterios:

Mínimo 1 letra mayúscula (sin acentos)

Mínimo 1 letra minúscula (sin acentos)

Un dígito (0-9)

Mínimo un carácter especial (No alfabético):

Caracteres válidos: @.\#&%()?/\;+!^\|:~}{<> \$*-+=

*Espacio no es carácter válido

- La contraseña debe cambiarse cada 60 días. Al pedir la contraseña de ingreso, si han pasado 60 días sin cambiar contraseña, debe solicitar cambio y después de cambiar, permitir el inicio de sesión (si el cambio de contraseña ha sido exitoso).



Ingreso de nueva contraseña. Dar clic en el botón **Verificar Contraseña** para ver el estado de la nueva contraseña ingresada (muy corta, débil, fuerte)

Funcionamiento de Editables

- En editables que no tienen registros, aparecerá el link **NEW** en el centro de la rejilla de datos.
- En editables que ya tienen registros creados, aparecerán los links: **EDIT**, **NEW** y **DELETE** junto a cada registro al lado izquierdo de la rejilla.

Nota: Pueden aparecer menos links según sea el diseño del editable.

- Después de diligenciada la información del editable, aparecerán después de las filas al lado izquierdo del formulario, los botones **UPDATE (guardar)** y **CANCEL**.

Nota: Los datos diligenciados en el editable deben tener el tamaño y tipo adecuado de acuerdo al campo, de lo contrario no se almacenará el nuevo registro. No es necesario diligenciar todos los campos del editable.

Complejidad de contraseña

Consola de administración Hawk y Cliente web

Si el usuario no ha cambiado contraseña va a solicitar cambio en el primer ingreso, la contraseña debe cumplir con las siguientes condiciones:

- La contraseña debe ser de mínimo 8 caracteres. El sistema recordará 10 últimas utilizadas para evitar que se repita.
- Debe incluir como mínimo 3 de los siguientes criterios:

Mínimo 1 letra mayúscula (sin acentos)

Mínimo 1 letra minúscula (sin acentos)

Un dígito (0-9)

Mínimo un carácter especial (No alfabético):

Caracteres válidos: @.\#&%()?/\;+!^|:~}{<> \$*-+=

*Espacio no es carácter válido

- La contraseña debe cambiarse cada 60 días. Al pedir la contraseña de ingreso, si han pasado 60 días sin cambiar contraseña, debe solicitar cambio y después de cambiar, permitir el inicio de sesión (si el cambio de contraseña ha sido exitoso).

Nota: Aplican los mismos criterios de seguridad de contraseña para usuarios del Cliente Web, aunque no hay restricción en cuanto a los caracteres permitidos.

Si se va a crear un nuevo usuario o editar la contraseña de un usuario existente aplican los mismos criterios de complejidad

Intel® Active Management Technology

Active Management Technology (Intel® AMT) – Tecnología para administración activa de Intel®

La incorporación de la tecnología AMT permite realizar tareas de diagnóstico y reparación remota de estaciones y servidores, aun cuando se encuentren fuera de banda. Intel AMT facilita la resolución de problemas y recuperación a distancia, por medio de las funciones de administración como el control remoto de teclado, video y mouse (KVM).

Requerimientos

- Esta tecnología viene integrada en:
[Familia de procesadores Intel® Core™ vPro™](#)
[Familias de procesadores Intel® Xeon® E5-2600, E5-1600 y E3-1200](#)
- Tarjetas de video y red integradas, se requiere que las dos sean integradas para que sea posible establecer la comunicación remota. El fabricante del equipo debe garantizar que todos los componentes soportan la tecnología Active Management (Intel® AMT)

Si se cumplen las condiciones anteriores:

- Habilitar **Intel® AMT- KVM** en las opciones de Bios.
[Ver Anexo. Ejemplo de configuración Intel® AMT - KVM](#)

Nota.

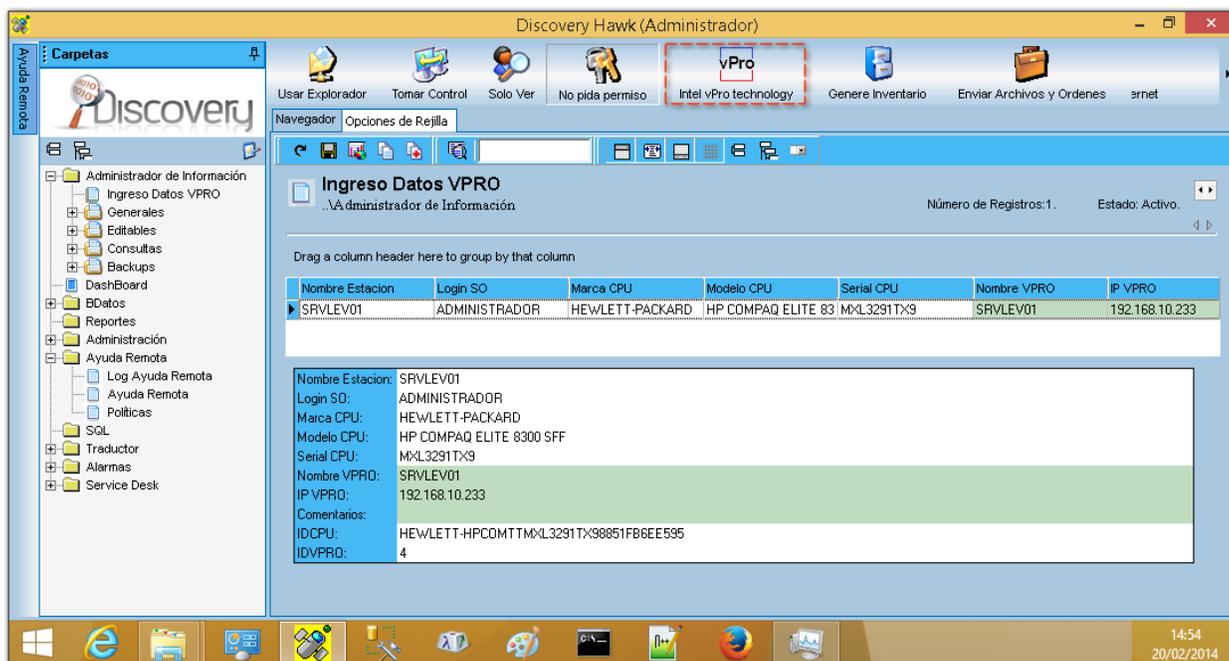
La configuración puede realizarse directamente en la Bios o con los aplicativos propios de Intel® para este propósito. Consultar la documentación Intel® según el tipo de hardware.

Cómo utilizar la tecnología Intel® AMT

Importante:

Habilitar el botón **Intel vPro Technology** (*Herramientas > Operaciones Remotas*) en el grupo (perfil) al que pertenece el administrador Discovery.

1. En la consola de administración Hawk, ubicar la vista editable **Ingreso datos VPRO**.
 Seleccionar la estación y dar clic en el botón **Intel vPro technology**



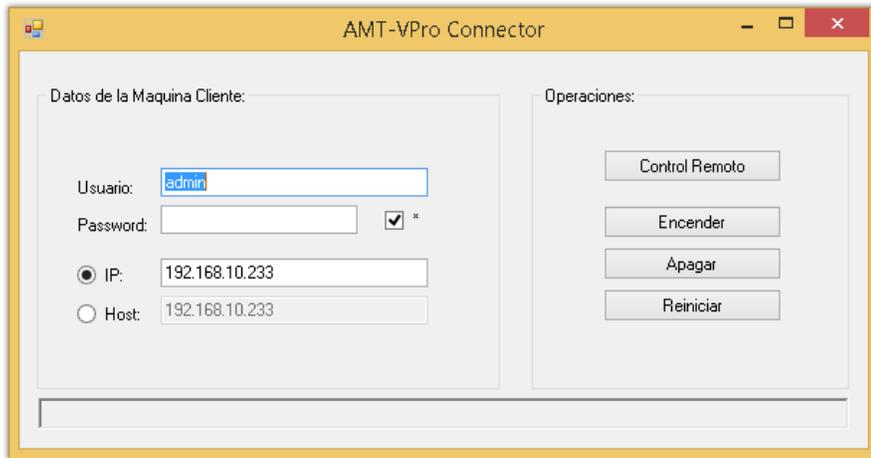
Se abrirá la subventana **AMT – Vpro Connector**

Ingresar los datos de usuario y **contraseña** para iniciar la sesión.

El usuario predeterminado es **admin**

La contraseña es la que se ha ingresado en la configuración AMT - KVM de la estación remota.

[Ver Anexo. Ejemplo de configuración Intel® AMT - KVM](#)

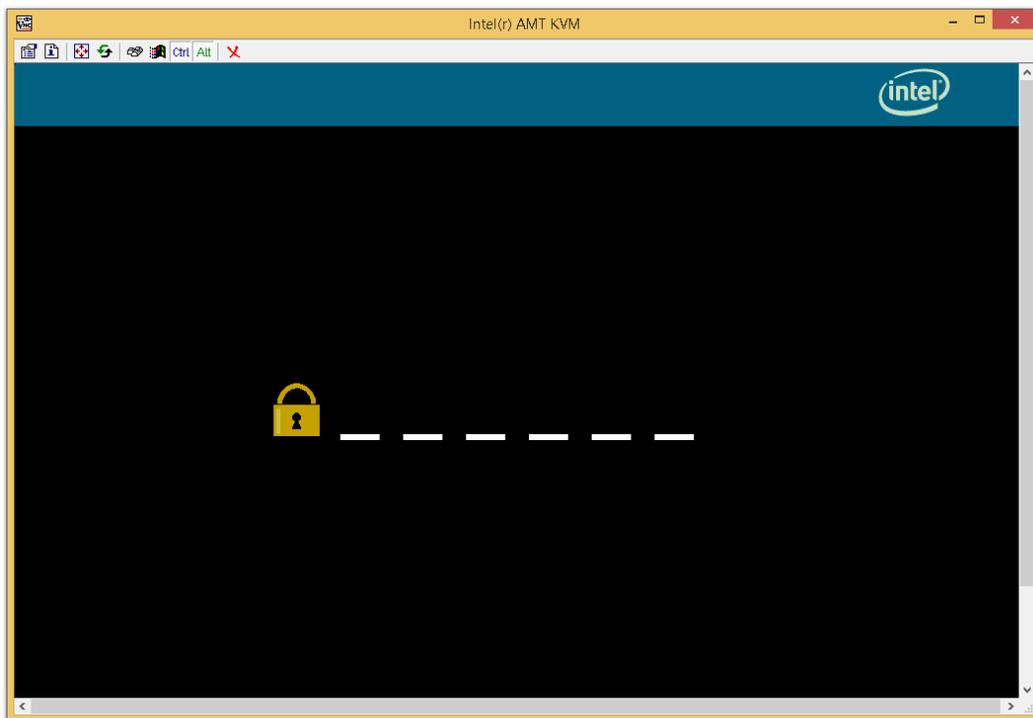


Operaciones disponibles:

Control Remoto

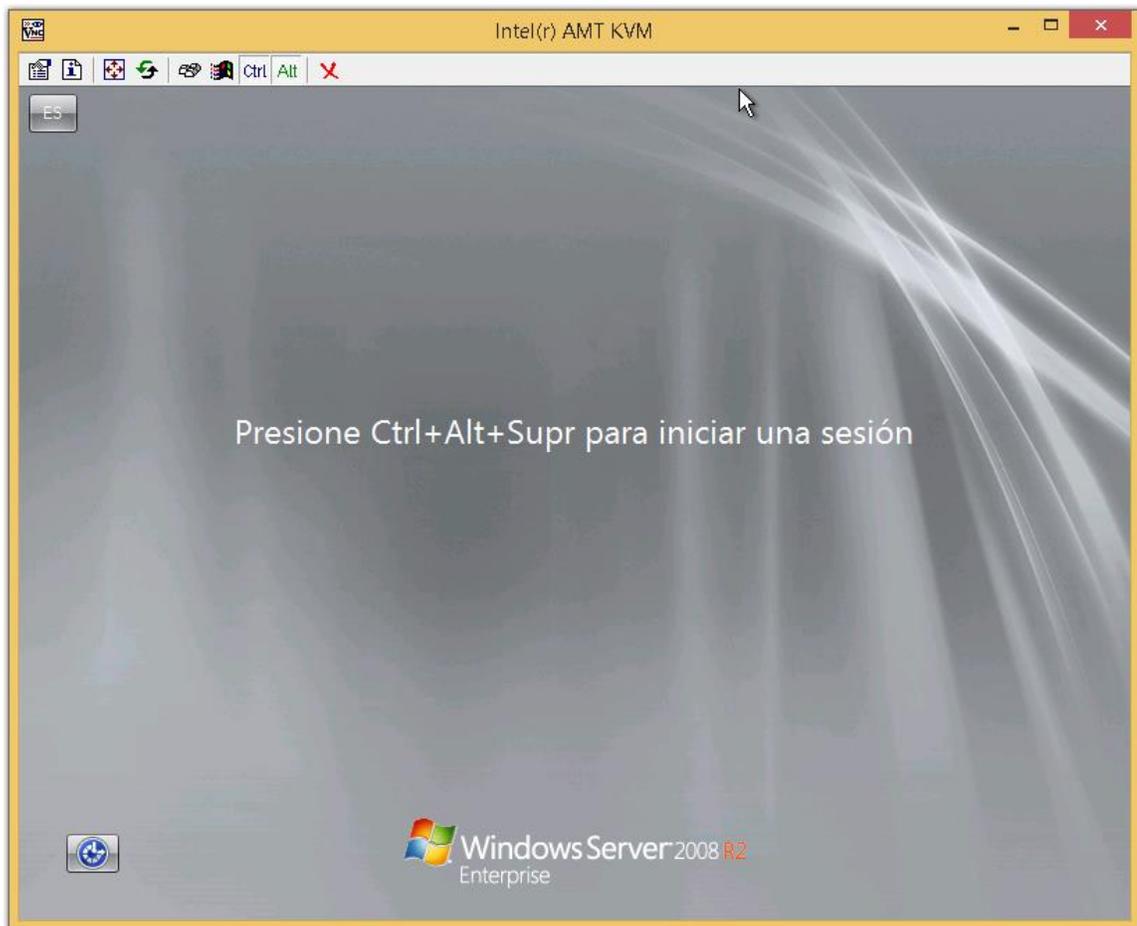
Prende el equipo remoto si está apagado y después lanza directamente la operación de control remoto. Si el AMT está configurado para que el usuario autorice la conexión ([Ver Anexo. Ejemplo de configuración Intel® AMT - KVM](#)) aparecerá una ventana con el mensaje de **conexión técnica** y un número de 6 dígitos que debe comunicarse al administrador Discovery¹ para que pueda establecer la conexión.

En la estación del administrador, aparecerá la siguiente ventana en la que se debe digitar el número de 6 dígitos proporcionado por el usuario de la estación remota:



¹ Usuario de la consola Discovery

Después de ingresar el número, pasa de forma automática la operación de Control Remoto:



Encender

Inicia el equipo remoto.

Reiniciar

Reinicia el equipo.

***No se reinicia el sistema operativo, el reinicio es directo al hardware

Apagar

Apaga el equipo remoto.

***No se reinicia el sistema operativo, el reinicio es directo al hardware

Importante: El AMT no apaga el sistema operativo sino el hardware directamente, por lo cual se recomienda programar el apagado del sistema a través del agente cuando sea posible. Utilizar los comandos propios del sistema operativo para el apagado seguro del sistema:

Windows Server 2008	Shutdown -p -f
Windows 8.1	Shutdown -p -f
Windows 7	Shutdown -p -f
Windows XP	Shutdown -s -f -t 0
Windows Server 2003	Shutdown -s -f -t 0

Módulo DRobot

Nuevo módulo para la administración de cuentas de correo, incluso cuentas que utilizan protocolo SSL². Cuenta con las funciones:

- **Email Reply:** Permite la transferencia de los correos de una cuenta de origen (POP3) a una cuenta destino (SMTP)
- **Email File:** Permite descargar los correos de una cuenta de correo origen (POP3), los correos descargados pueden ser procesados por el sistema con la nueva función del SchedulerTask: Verificar por archivo

Creación de cuentas de correo

1. Cargar la información por defecto en la base de datos para el módulo DRobot*: [Ver Módulo SetupBox](#)
* Aplica para el caso de instalaciones previas. La base de datos del instalador n9 ya incluye la información por defecto.

2. Abrir el módulo ServiceManager.exe
En el servidor Discovery abrir el *DRobot*, dar clic derecho sobre el icono  en el área de notificaciones de la barra de tareas del escritorio y seleccionar la opción **Abrir**.

Ubicación del aplicativo:

<unidad>:\Program Files\LeverIT\Discovery\Software\SrvPrg\ServiceManager.exe

Desplegar el nodo Servicios y seleccionar la opción **Administración**. Habilitar la casilla **Activar**, ésta casilla habilita la función de verificación del módulo DRobot, monitorea que se encuentre activo en intervalos de tiempo de 60 segundos, en caso de que el DRobot no esté activo lo reiniciará automáticamente.

Abrir el módulo DRobot.exe

En el servidor Discovery abrir el *DRobot*, dar clic derecho sobre el icono  en el área de notificaciones de la barra de tareas del escritorio y seleccionar la opción **Abrir**.

Ubicación del aplicativo:

<unidad>:\Program Files\LeverIT\Discovery\Software\SrvPrg\DRobot.exe

3. Desplegar el nodo *Email > Configuración* y dar clic en la opción **Cuentas**
En el panel izquierdo ingresar el nombre de la cuenta y dar clic en el botón **+Pop3³** o **+Smt⁴**, de acuerdo al tipo de cuenta.
4. En el panel derecho agregar los atributos de la cuenta:
 - **Proveedor:** En el campo de lista seleccionar el proveedor del servicio.
Por defecto: Outlook, Yahoo, Gmail o None (para cuentas de diferentes servidores).
Después de la selección, dar clic en el botón 
Agrega la configuración por defecto según el tipo de cuenta y proveedor del servicio.
 - **Nombre del Servidor:** Nombre del servidor de correo. Ej.: pop3.live.com

² **SSL.** Protocolo de conexión segura por Internet

³ **POP3.** El **protocolo POP** (*Protocolo de oficina de correos*), como su nombre lo indica, permite recoger el correo electrónico en un servidor remoto (servidor POP).

⁴ **SMTP.** El **protocolo SMTP** (*Protocolo simple de transferencia de correo*) es el protocolo estándar que permite la transferencia de correo de un servidor a otro mediante una conexión punto a punto.

- **Método:** Tipo de autenticación en el servidor, incluye métodos como CRAM-MD5, DIGEST-MD5, NTLM, etc. Se recomienda utilizar la opción por defecto **Auto**.

Nota: Si se requiere utilizar otro método de autenticación diferente a *Auto*, verificar si es soportado por el servidor y las opciones de configuración (puerto, seguridad, etc.) requeridas.

- **Puerto Servidor:** Número de puerto del servicio.
- **Seguridad:** Tipo de seguridad que se utilizará en la conexión con el servidor. Opciones posibles:

Implicit: Con *SSL implícito*, tanto el cliente como el servidor utilizarán el protocolo SSL durante toda la sesión. El cliente se conecta e intenta establecer una conexión segura (SSL handshake) y si es exitosa la comunicación segura continúa durante la sesión. Por esta razón, el SSL implícito típicamente usa un puerto diferente al habitualmente utilizado por el protocolo. Por ejemplo el puerto 995 es el comúnmente utilizado por POP con el protocolo SSL.

Explicit: Con *SSL Explícito*, la comunicación segura se establece solo hasta que se efectúa previamente la negociación con el servidor. El cliente se conecta normalmente al servidor por el puerto utilizado habitualmente por el protocolo y expide entonces el comando STARTTLS. Si el servidor soporta este mecanismo y responde positivamente, la comunicación segura continuará por el resto de la sesión.

Otros tipos: *Unsecured y Tumbleweed tunnel*

Por defecto el módulo utiliza los tipos:

Implicit para el protocolo POP3, puerto 995

Explicit para el protocolo SMTP, puerto 587

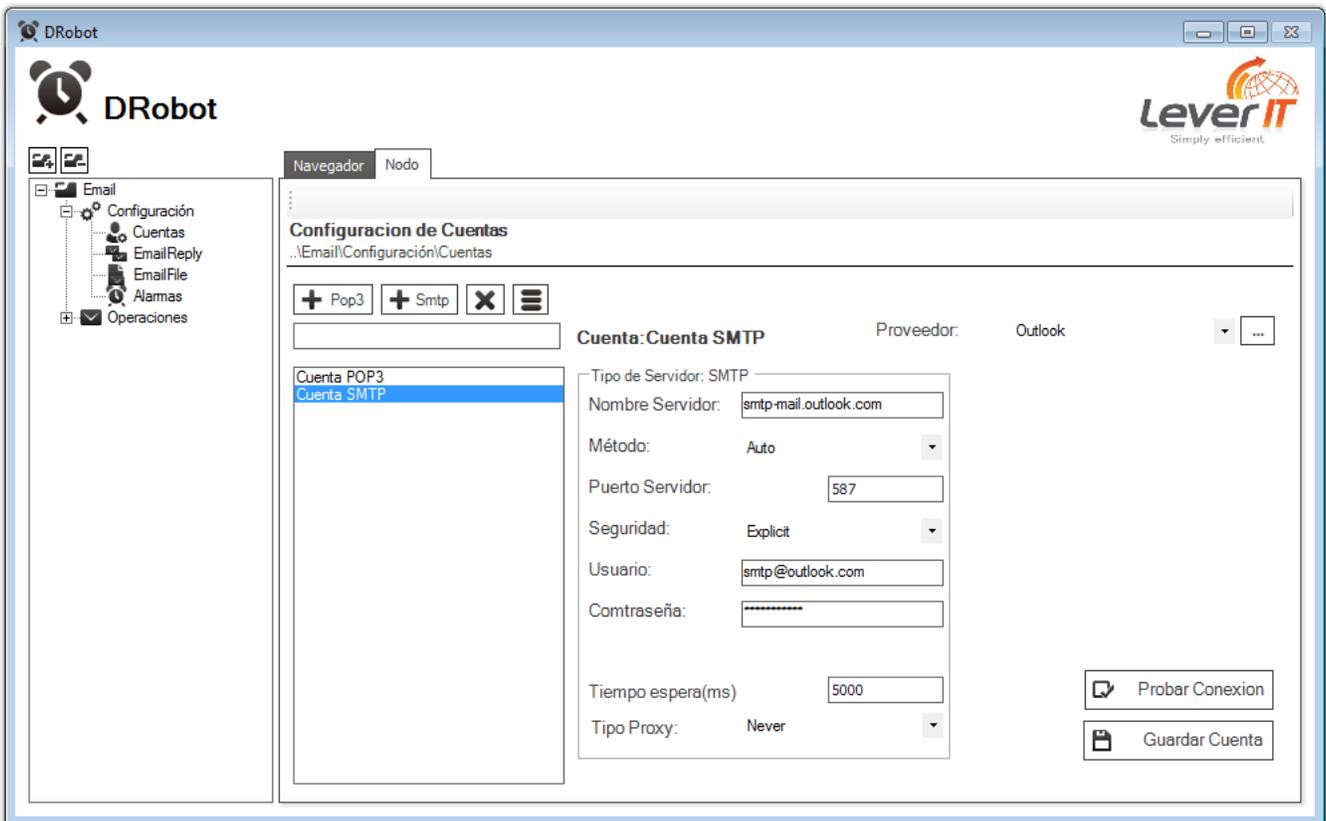
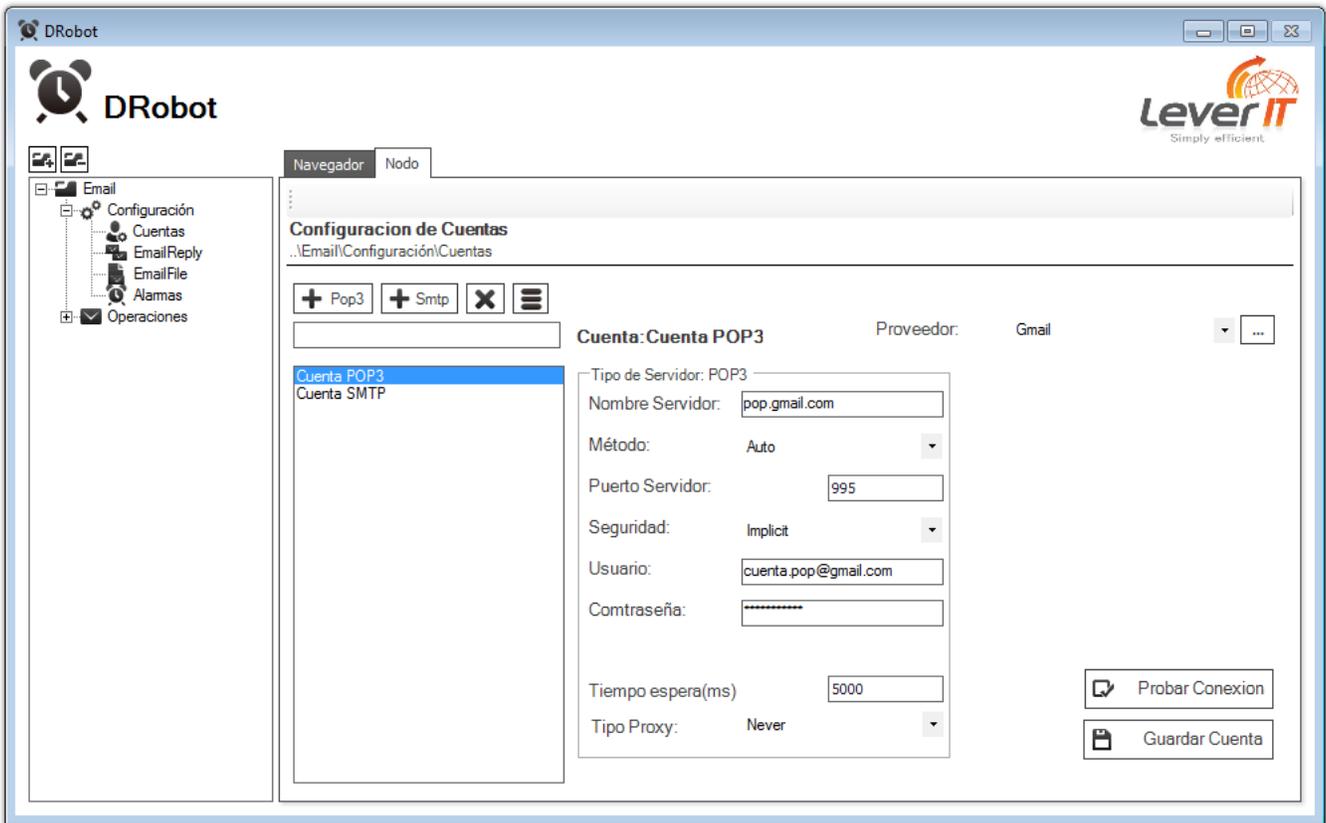
- **Usuario:** Cuenta de correo.
- **Contraseña:** Contraseña de la cuenta de correo.
- **Tiempo Espera (ms):** Tiempo para reconexión con el servidor, por defecto: 5000ms.
- **Tipo Proxy:** Listado de protocolos en caso de utilizar servidor Proxy. Incluye los protocolos Socks (4, 4A, 5) y HttpConnect.

Si se selecciona alguno de los protocolos se activarán los campos para configuración de Proxy en el panel a la izquierda:

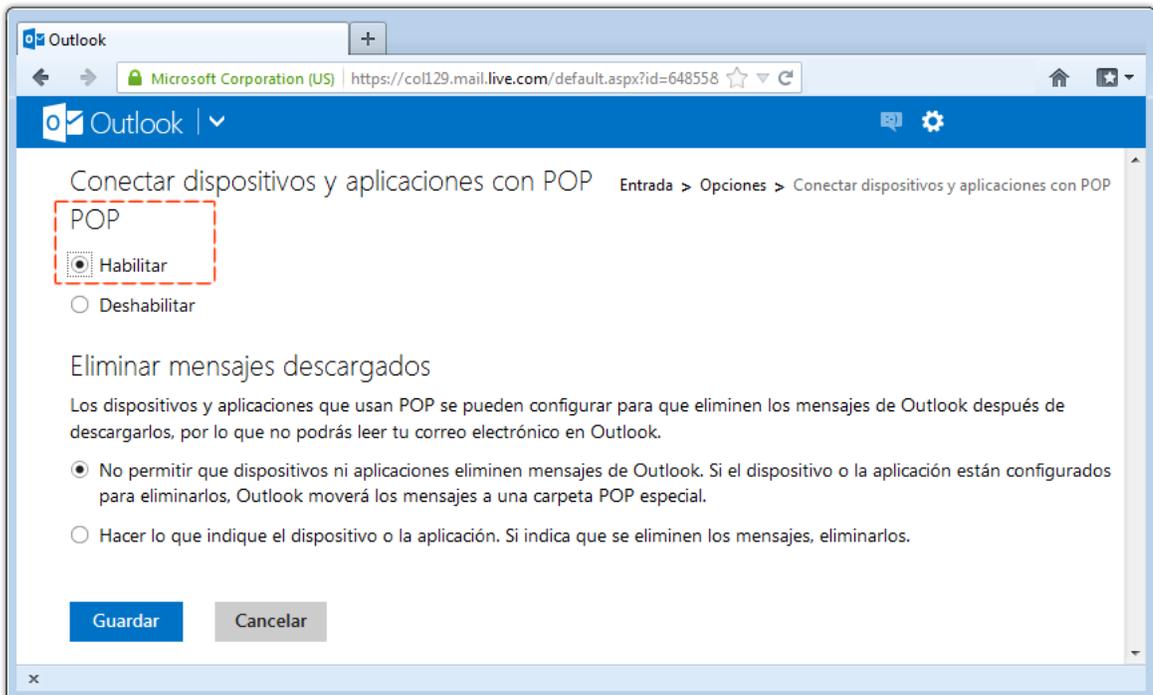
The image shows a 'Proxy Settings' form with the following fields: 'Servidor', 'Puerto' (with '0' entered), 'Usuario', 'Contraseña', 'Método' (a dropdown menu currently showing 'Basic'), and 'Dominio'. A red rectangular box highlights the 'Método' dropdown. A red arrow points from the text 'Se activa en caso de utilizar el protocolo HttpConnect' to the 'Método' dropdown.

Nota: Si se ha seleccionado None como proveedor del servicio, ingresar de forma manual los demás atributos de la cuenta.

5. Dar clic en el botón **Probar Conexión**, la prueba de verificación debe ser exitosa, de lo contrario, corregir los atributos de la cuenta. Finalmente dar clic en el botón **Guardar Cuenta**.



Importante: En la configuración de las cuentas POP3, debe estar habilitada la opción POP.



Programación de ejecución

1. Abrir el módulo DRobot y desplegar el nodo *Email > Configuración* y dar clic en la opción **Alarmas**.
2. En el campo de texto ingresar el nombre de la alarma y dar clic en el botón 
3. Seleccionar la cuenta y en Días de ejecución, habilitar los días en los que se ejecutará la tarea. (Email File, Email Reply).
4. Definición de tiempos:

Hora inicial: Editar la hora en que empezará la tarea Email File o Email Reply.
Formato de hora HH:MM:SS (Formato 24 horas).

Hora final: Editar la hora en que terminará la tarea Email File o Email Reply.
Formato de hora HH:MM:SS (Formato 24 horas).

Intervalo: Frecuencia de ejecución de la tarea, dentro del periodo de tiempo definido entre la hora inicial y final configuradas.

5. Para finalizar, dar clic en el botón **Guardar**.

Función Email Reply

1. Abrir el módulo DRobot y desplegar el nodo *Email > Configuración* y dar clic en la opción **EmailReply**.
2. En el campo de texto ingresar el nombre de la tarea y dar clic en el botón
3. Con la tarea seleccionada, en el panel *Cuenta*, configurar:

Origen: Listado con las cuentas de tipo POP3 creadas previamente. Seleccionar la cuenta desde la que se enviarán los correos.

Destino: listado con las cuentas de tipo SMTP creadas previamente. Seleccionar la cuenta a la que serán enviados los correos.

Alarma: Listado con las alarmas creadas. Seleccionar la alarma para programar la ejecución de la tarea.

Borrar Email: Habilita/deshabilita la función de eliminación de correos del buzón origen. El borrado en el buzón origen se realizará solo al terminar el reenvío de todos los correos al servidor Discovery. Se recomienda habilitar esta función ya que según sea la configuración de la alarma de ejecución podría enviarse repetidamente el contenido del buzón de correo origen.

4. Proceso de reenvío

Los correos serán descargados temporalmente al servidor Discovery a un subdirectorio, en la siguiente ubicación: `<unidad>:\Program Files\LeverIT\Discovery\Email\Reply\1*`
*# Tarea Email Reply

Por cada tarea se creará un subdirectorio. Los archivos de correo tendrán la extensión **eML**. Cuando termine de descargarse el contenido del buzón origen al servidor Discovery empezará el reenvío a la cuenta SMTP configurada en la tarea.

5. Dar clic en el botón **Guardar**.

Nota: Imágenes, texto enriquecido, y adjuntos no serán procesados, por lo que en el reenvío se perderán esas características del correo original.

Función Email File

1. Abrir el módulo DRobot y desplegar el nodo *Email > Operaciones* y dar clic en la opción **EmailFile**.
2. Con la tarea seleccionada, en el panel *Cuenta*, configurar:

Origen: Listado con las cuentas de tipo POP3 creadas previamente. Seleccionar la cuenta de la que se descargarán los correos al servidor Discovery.

Alarma: Listado con las alarmas creadas. Seleccionar la alarma para programar la ejecución de la tarea.

Borrar Email: Habilita/deshabilita la función de eliminación de correos del buzón origen. El borrado en el buzón origen se realizará solo al terminar el reenvío de todos los correos al servidor Discovery. Se recomienda habilitar esta función ya que según sea la configuración de la alarma de ejecución podría enviarse repetidamente el contenido del buzón de correo origen.

3. Proceso de Recepción

Cuando los correos de la cuenta origen se descarguen al servidor Discovery, se almacenarán temporalmente en el siguiente subdirectorio:

`<unidad>:\Program Files\LeverIT\Discovery\Email\Incoming`

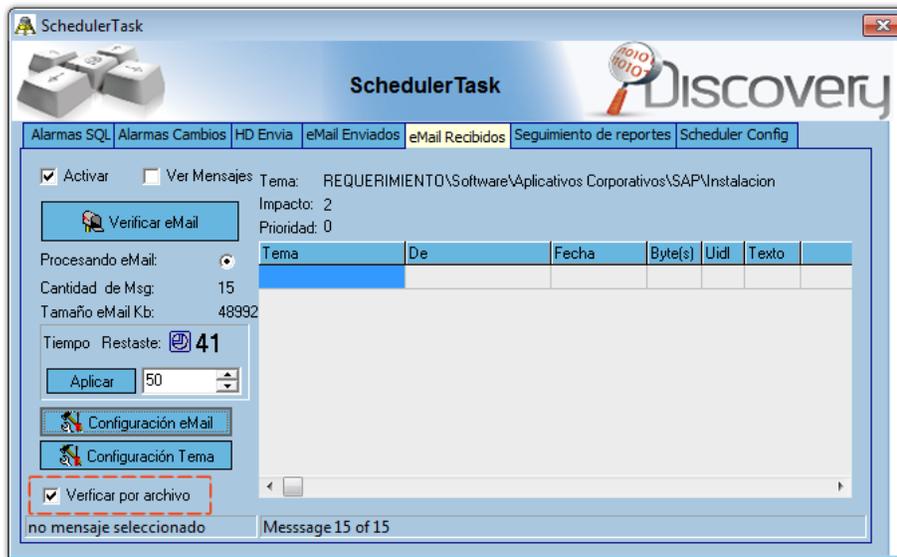
Los archivos almacenados en este subdirectorio tendrán extensión **emi**.

Para que los correos sean procesados por el SchedulerTask y Datanor e ingresen como nuevos reportes:

Abrir el SchedulerTask y seleccionar la pestaña *eMail Recibidos*, en esta ventana habilitar la casilla **Verificar por archivo** (por defecto activa). Previamente deben estar configurados el tema y urgencia para recepción de tickets por email. Cuando está activa la casilla Verificar por archivo no serán procesados los correos de la cuenta configurada en la pestaña *Recibir eMail (POP3)*.

Cuando termine el reenvío de todos los correos al servidor, comenzará el procesamiento y a medida que se procesen los archivos y se creen los nuevos tickets se eliminarán de forma automática del directorio.

Nota: Los archivos que no puedan ser procesados como tickets serán igualmente eliminados del directorio Incoming. Imágenes, texto enriquecido, y adjuntos no serán procesados en los nuevos tickets. Puede habilitarse la opción **Asunto a eMail a incluir**, no es necesario que se habilite una cuenta POP3.



Monitoreo de operaciones

1. Abrir el módulo DRobot y desplegar el nodo *Email > Operaciones* y dar clic en **Disparador**.
2. En esta vista se pueden visualizar el estado de las tareas **Email File**, **Email Reply**. Si se deshabilita la casilla **Activo**, no será procesada ninguna de las tareas.
Ver Msg Comunic: Habilita/deshabilita los mensajes de estado de las tareas, se recomienda deshabilitar.

DRobot

Estado del Disparador
..Email\Operaciones\Disparador

Recarga y Verifica

Ver Msg Comunic

Activo 26

Alarmas Pendientes: 0

Listo

19/385 Descargado(s)

#	Disparador	Tipo	Fecha	Asunto	Detalle
8	Diaria	_File	31/07/2014 03:57:09 p.m.	--	--
7	Diaria	_File	31/07/2014 03:56:02 p.m.	--	--
6	Diaria	_Reply	31/07/2014 03:30:34 p.m.	--	--
5	Diaria	_Reply	31/07/2014 03:30:34 p.m.	--	--
4	Diaria	_Reply	31/07/2014 03:29:32 p.m.	--	--
3	Diaria	_Reply	31/07/2014 03:29:32 p.m.	--	--
2	Diaria	_Reply	31/07/2014 03:28:25 p.m.	--	--
1	Diaria	_Reply	31/07/2014 03:28:25 p.m.	--	--

Módulo ServiceManager

Nuevo módulo que inicia y monitorea (cada 60 seg.) el servicio DRobot y permite la visualización de:

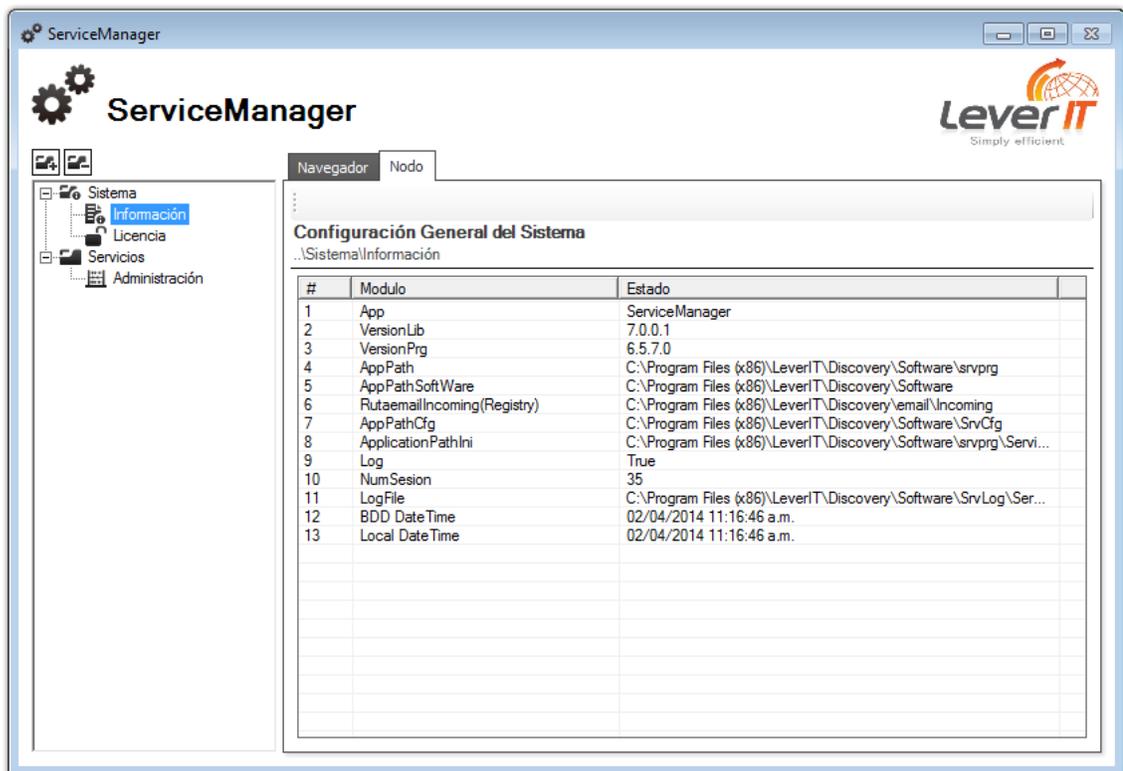
- Información básica del servidor: Rutas de instalación, versión, formato de fecha de base de datos y del servidor Discovery, etc.
- Tipo de licencia: Validez del serial, número de licencias, editables, administradores y visores.

Abrir el módulo ServiceManager.exe

En el servidor Discovery abrir el *ServiceManager*, dar clic derecho sobre el icono  en el área de notificaciones de la barra de tareas del escritorio y seleccionar la opción **Abrir**.

Ubicación del aplicativo:

<unidad>:\Program Files\LeverIT\Discovery\Software\SrvPrg\ServiceManager.exe



Desplegar el nodo *Servicios* y seleccionar la opción **Administración**. Habilitar la casilla **Activar**, ésta casilla habilita la función de verificación del módulo DRobot, monitorea que se encuentre activo en intervalos de tiempo de 60 segundos, en caso de que el DRobot no esté activo lo reiniciará automáticamente.

Módulo SetupBox

Nuevo módulo que permite la creación y configuración inicial para el servicio DRobot. Incluye también información del sistema y licencia, al igual que el módulo ServiceManager.

Para cargar las tablas e información para funcionamiento del módulo DRobot:

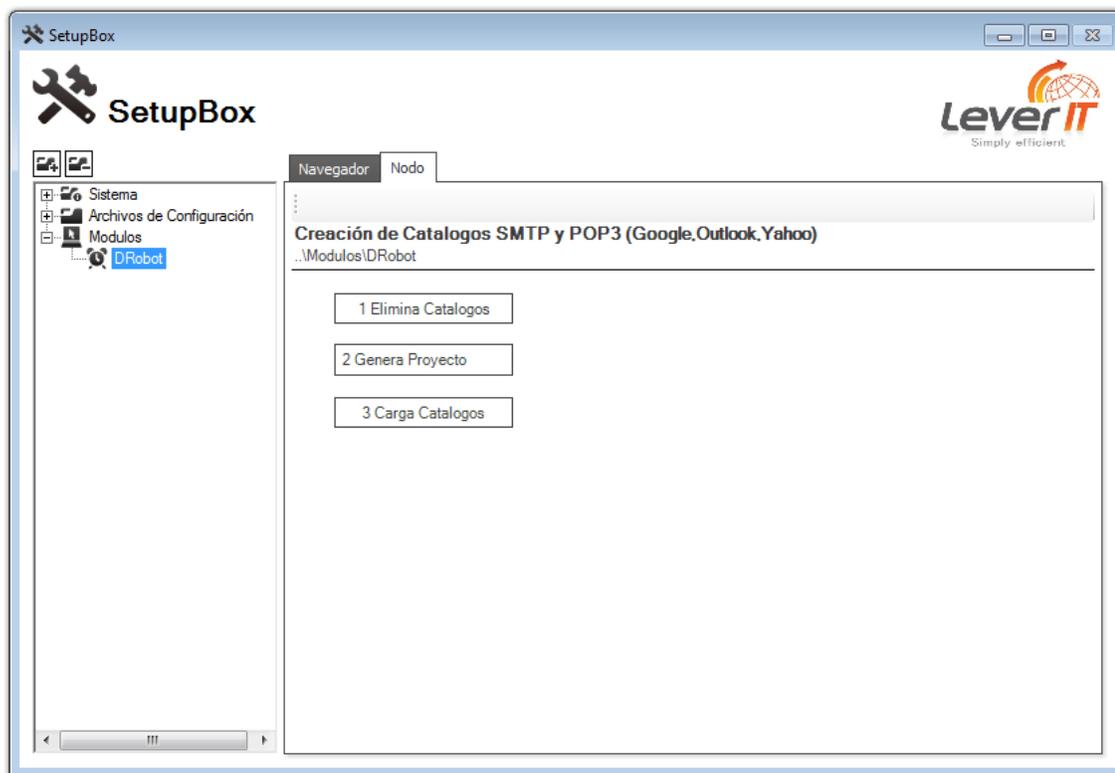
1. Abrir el módulo SetupBox.exe

Ubicación del aplicativo:

<unidad>:\Program Files\LeverIT\Discovery\Software\SrvPrg\SetupBox.exe

2. Abrir el nodo *Módulos* y seleccionar **DRobot**:

- Para la creación de las nuevas tablas que requiere el módulo: Dar clic en el botón **Genera Proyecto**
- Para cargar la información por defecto (proveedor, puerto, seguridad, etc): Dar clic en el botón **Carga Catálogos**
- Para eliminar las nuevas tablas: Dar clic en el botón **Elimina Catálogos**.



Otros cambios

- Mejora en el proceso de conexión de operaciones remotas de versión Global
- Mejora en resolución del control remoto por internet. Resolución igual a la conexión LAN
- Mejora para detección de uso de software. Nueva tabla USO_MULTI_SOFT

Para sistemas Windows:

- Mejora control remoto para sistemas Windows 8
- Mejora para detección de sistemas Windows 8.1
- Registro de eventos de encendido, apagado y crash de estaciones Windows. Nueva tabla EVENTONOFF

Nuevos parámetros para configuración de EVENTONOFF y mejora en Auditoría de Archivos

Para activar EVENTONOFF:

La nueva función lee del visor de eventos para poder alimentar la fecha y el tipo de evento según sea.

Requiere la creación manual del archivo DISC.CFG e incluir el parámetro EVENTONOFF=1. Se registrará la información de los últimos 30 días.

Para activar USO_MULTI_SOFT:

Requiere la creación manual del archivo DISC.CFG e incluir el parámetro AUDITDAYS=1, para que se generen múltiples inventarios día por día hasta la fecha actual - 1 (Ayer). La información que se logre recopilar por cada día se almacena en la tabla USO_MULTI_SOFT.

Para sistemas Mac:

- Mejora en captura inventario
- Reducción en tiempo de generación de inventarios
- Nueva ventana para solicitud de permiso al usuario para Control Remoto. Soporte desde versión 10.6 a 10.9. Tiempo espera respuesta de 20 seg.
- Nuevo archivo: agentpi.exe para soporte de ventana permiso control remoto. Usa puerto TCP 17020
- Nueva función para generación de inventario cada 4 horas (únicamente para equipos Mac/Linux)

Para sistemas Android:

- Soporte de idioma (Ingles / Español) para instalación de APK Android
- Ajuste en parámetro de seguridad para instalación del APK en sistemas Android 4.3

Comandos:

- Nuevo CMD:44 para cambiar el atributo de archivo a lectura/escritura

Ej.:

CMD:44

C:\TEMP\NOTA.XLS

--

- Nuevo CMD:45 para solicitar uso de software de un día específico

Ej.:

CMD:45

NUMERO*

--

***NÚMERO:** Es el valor del día, teniendo como referencia el número 16077 que corresponde al 7 de enero de 2014. Ej.: 16078 representa el 8 de enero de 2014, 16079 representa el 9 de enero de 2014. Cuando se envía este comando, el agente en la estación verifica sus archivos de uso de software y toma las estadísticas de uso de ese día únicamente y las envía en un inventario que solo trae la información solicitada para la tabla USO_MULTI_SOFT.

- Nuevo CMD:46 para ejecución de tareas secuenciales

CMD:46

TYP:ttt

RES:rrr

EXE:eee

PAR:ppp

FIN:fff

OUT:ooo

Donde

TYP:ttt: Es un número cuyos valores pueden ser: 0 1 2 o 3.

0 Indica que no se utilizarán los parámetros de salida ni entrada.

1 indica que se re direccionará el archivo de entrada al stdin del exe, 2 que se re direccionará la salida al archivo de salida fff.

2 Indica que se utilizará el parámetro de salida únicamente.

3 Indica que se utilizarán los dos parámetros, salida y entrada.

RES:rrr: Es un número cuyos valor puede ser: 0 o 1. 1 indica que se analizará el valor definido en ppp y si se encuentra algún ~ se cambiará por la ruta donde se descomprimió el archivo. 0 es el valor por defecto de ruta que se indique en la variable.

EXE:eee: Es la ruta de ubicación del ejecutable. Si existe el carácter ~ se cambia por la ruta donde se abrió el zip.

PAR:ppp: Son los parámetros con los que se ejecutara el programa.

FIN:fff: Es la ruta del archivo de entrada.

OUT:ooo: Es la ruta del archivo de salida.

Ej.:

CMD:1

INICIA Y SIGUE CMD 46 con Instalación Silenciosa Visor PowerPoint

CMD:46

TYP:3

RES:0

EXE:cmd.exe

PAR:/K E:\PowerPointViewer2010Esp.exe /quiet

FIN:

OUT:E:\F_OUT.TXT

CMD:1

TERMINA CMD

--

Anexo

Ejemplo de configuración de Intel® AMT - KVM

Importante: Las opciones de menú y de configuración para la configuración de la tecnología Intel® AMT – KVM pueden cambiar según el hardware, marca, modelo y versión de Bios. Consultar la información propia del fabricante para realizar la configuración necesaria.

1. Habilitar la opción **Firmware Verbosity (O Boot Verbosity)** en la Bios. Reiniciar el equipo, debe aparecer el menú que permite el ingreso a la extensión para administración **Intel® (Intel® MEBx)**.

```
Intel(R) Management Engine BIOS Extension v2.5.15.0000
Copyright (C) 2003-06 Intel Corporation. All Rights Reserved.

Firmware Version Matched ...
Press <CTRL-P> to enter Intel(R) ME Setup
```

Si el AMT nunca se ha configurado en el equipo se solicitara una contraseña para ingresar, digitar *admin* (contraseña por defecto), después aparecerá de forma automática un mensaje solicitando la creación de una nueva contraseña.

Reglas para la creación de la contraseña:

- Puede tener entre 8 y 32 caracteres de longitud

Importante: Con Discovery como servidor de AMT, se requiere que el password cumpla con los criterios de creación de contraseña en los primeros 8 caracteres. Ej.: P@ssw0rd

- Debe contener letras mayúsculas y minúsculas (**A, a, B, b**)
- Debe contener al menos un carácter numérico (**0-9**)
- Al menos un carácter ASCII 7-bit que no sea alfanumérico (**@,#,!,\$,%,***), con un valor ASCII entre 33d y 126d

'_' el carácter underscore se considera alfanumérico

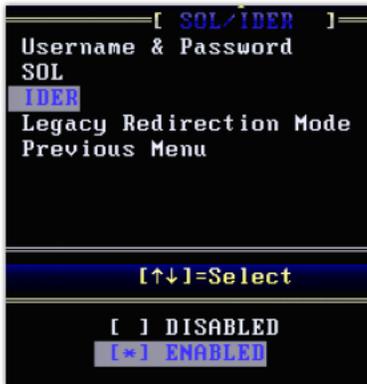
Los siguientes caracteres no son válidos: " , ' < , > , : , & , espacio

2. Ingresar al motor de administración **Intel® (Intel ME)**.
 Seleccionar el menú *Intel ME General Settings > Network Setup > Intel ME Network Name Settings*
 Ingresar el nombre del equipo (hostname) y el nombre del domino al que pertenece.
3. Salir al menú previo *Intel ME General Settings* y seleccionar la opción **Active Network Access**, al seleccionar esta opción aparecerá un mensaje de confirmación de activación de la interfaz de red ME:

```
[Caution]
Activates the current network settings
and opens the ME network interface
Continue: (Y/N)
```

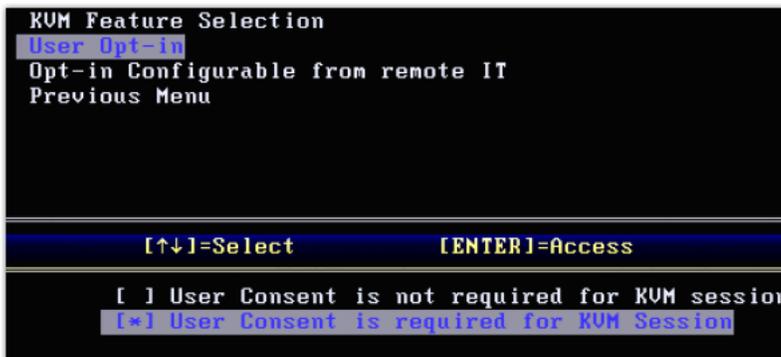
Guardar los cambios realizados.

4. Regresar al menú principal, seleccionar la opción **Manageability feature selection**. Y verificar que esta opción se encuentra activa. En el mismo menú escoger **SOL/IDER**, verificar que las opciones **SOL**, **IDER**, y **Legacy Redirection Mode** están habilitadas.

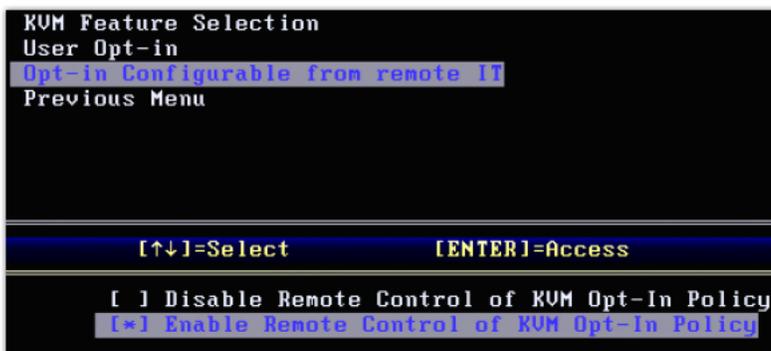


5. Volver al menú **Intel® AMT Configuration** y seleccionar la opción **KVM Configuration**. Verificar que la opción **KVM Feature Selection** está habilitada.

En este mismo menú se encuentra la opción **Opt-in** que habilita o deshabilita el consentimiento del usuario para iniciar la sesión KVM.



Después habilitar la opción **Opt - in Configurable from remote IT**



6. Guardar los cambios realizados y continuar con el encendido de la máquina.



www.leverit.com
Contacto: info@leverit.com

SOPORTE TÉCNICO INTERNACIONAL