COE Modernización del Datacenter - ATAIS



Guía de Operaciones

Preparado para

Nombre del cliente

noviembre 14, 2016

Versión 1 Borrador

Preparado por

**Mario Inostroza**

Senior Consultant

marioi@microsoft.com

Hoja de revisión y aprobación

Registro de cambios

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Autor | Versión | Referencia del cambio |
| 8/11/2016 | Mario Inostroza | 1 | Borrador inicial para revisión y discusión |
|  |  |  |  |
|  |  |  |  |

Revisores

|  |  |  |  |
| --- | --- | --- | --- |
| Nombres | Versión aprobada | Cargo | Fecha |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabla de contenido

[1 Resumen de guía de operaciones 1](#_Toc466393569)

[2 Consola de detección de amenazas 4](#_Toc466393570)

[3 Modificación de la configuración del Centro ATA 7](#_Toc466393571)

[4 Modificación de la configuración de la puerta de enlace de ATA 15](#_Toc466393572)

[5 Alertas de ATA 17](#_Toc466393573)

[6 Centro de mantenimiento de ATA 22](#_Toc466393574)

[7 Actividades sospechosas 23](#_Toc466393575)

[8 Configuración de detección de ATA 27](#_Toc466393576)

[9 Base de datos de ATA 28](#_Toc466393577)

[10 Validación de creación de reflejo del puerto 30](#_Toc466393578)

[11 Configuración de retroalimentación de ATA para Microsoft 33](#_Toc466393579)

## Tablas

[Tabla 1: Resumen de tareas 1](#_Toc466393580)

[Tabla 2: Habilidades requeridas y recomendaciones 2](#_Toc466393581)

[Tabla 3: Elementos de la consola 5](#_Toc466393582)

[Tabla 4: Fases de modificación de dirección IP—Centro 7](#_Toc466393583)

[Tabla 5: Actualización del certificado—Centro ATA 9](#_Toc466393584)

[Tabla 6: Configuración de alertas por correo electrónico 19](#_Toc466393585)

[Tabla 7: Gravedad de actividades sospechosas 24](#_Toc466393586)

[Tabla 8: Estado de las actividades sospechosas 25](#_Toc466393587)

[Tabla 9: Opciones de configuración de detección 27](#_Toc466393588)

1. Resumen de guía de operaciones

Este documento lista todas las actividades de operaciones para Microsoft Advanced Threat Analytics (ATA) y explica cuándo debe BCI realizar estas actividades. También considera el plan de negocios como parte de las operaciones para este proyecto.

Este documento supone que ATA ya se ha instalado y configurado, y está ejecutándose correctamente en el entorno de BCI. Este documento no cubre la instalación, configuración o diagnóstico de fallas de ATA. Cubre lo que un administrador de ATA debe comprobar cada día, semana, mes y trimestre para ayudar a que ATA se ejecute de la manera esperada.

* 1. Objetivos

Los objetivos de este documento son asesorar a BCI para que opere, administre y gestione de manera eficaz la solución de ATA que se implemente en este proyecto.

Se cubren los siguientes temas como parte de las operaciones de ATA:

* Trabajar con la consola de ATA
* Modificar la configuración de ATA
* Trabajar con las alertas de ATA
* Centro de mantenimiento de ATA
* Trabajar con actividades sospechosas
* Trabajar con configuraciones de detección de ATA
* Administración de bases de datos de ATA
* Administrar configuración de telemetría
  1. Resumen de tareas

La siguiente tabla lista todas las tareas administrativas tratadas en esta guía y la frecuencia con que deben realizarse.

Tabla 1: Resumen de tareas

| Nombre de la tarea | Frecuencia |
| --- | --- |
| Supervisión del panel | A diario |
| Trabajar con actividades sospechosas | A diario |
| Revisar alertas en el panel | A diario |
| Supervisar uso de memoria (centro y puerta de enlace) | A diario |
| Revisar registros de desempeño y alertas | Semanal |
| Actualizaciones de seguridad para los servidores | Mensual |
| Análisis de directivas y de configuración | Trimestral |
| Modificaciones de revisión de alertas | Cuando sea necesario |
| Revisar y actualizar el plan de respuesta | Cuando sea necesario |
| Cambiar configuración de ATA | Cuando sea necesario |
| Hacer copias de seguridad, mover o restaurar las bases de datos de ATA | Cuando sea necesario |
| Administrar membresía de grupos de seguridad | Cuando sea necesario |
| Validación de creación de reflejo del puerto | Cuando sea necesario |

* 1. Requisitos de habilidades

Para operar la solución de ATA implementada en el entorno de BCI como parte de este proyecto, se prefieren las siguientes habilidades. Esta recomendación es aplicable a una combinación de equipos o de individuos.

Tabla 2: Habilidades requeridas y recomendaciones

| Rol | Descripción |
| --- | --- |
| Equipo de detección de amenazas | Este equipo es responsable de realizar el análisis y la revisión de amenazas. |
| Equipo de respuesta a amenazas | Este equipo es responsable de responder a un indicador de amenaza que descubra el equipo de detección de amenazas. |
| Equipos de administración de redes | Este equipo configura la creación de reflejos de puertos en la red física y en las redes virtuales ubicadas en los hosts virtuales. |
| Individuos con conocimientos sobre la detección y respuesta a las amenazas | Estos individuos entienden qué son amenazas para la empresa y cómo identificarlas; además tienen el conocimiento efectivo de los procesos de respuesta requeridos para responder a las amenazas identificadas. |
| Individuos con conocimientos sobre creación de reflejos de puertos | Tener a estos individuos en el equipo sería una ventaja. Por lo general, la creación de reflejos de puertos es responsabilidad de los equipos de administración de redes dedicados. |
| Individuos con experiencia en certificados X.509 | Es obligatorio un buen entendimiento de la infraestructura de claves públicas y los certificados de terceros. Esto es necesario con la solicitud, importación, exportación y transferencia de certificados entre el centro y la puerta de enlace. |

1. Consola de detección de amenazas

Cualquier usuario que sea miembro del grupo de Administradores locales en el servidor del Centro ATA tiene permiso de iniciar sesión en la Consola de ATA y administrar la configuración de ATA. Para que un usuario pueda iniciar sesión en la Consola de ATA sin que sea administrador local, agréguelo al grupo local: **Administradores de Microsoft Advanced Threat Analytics.**

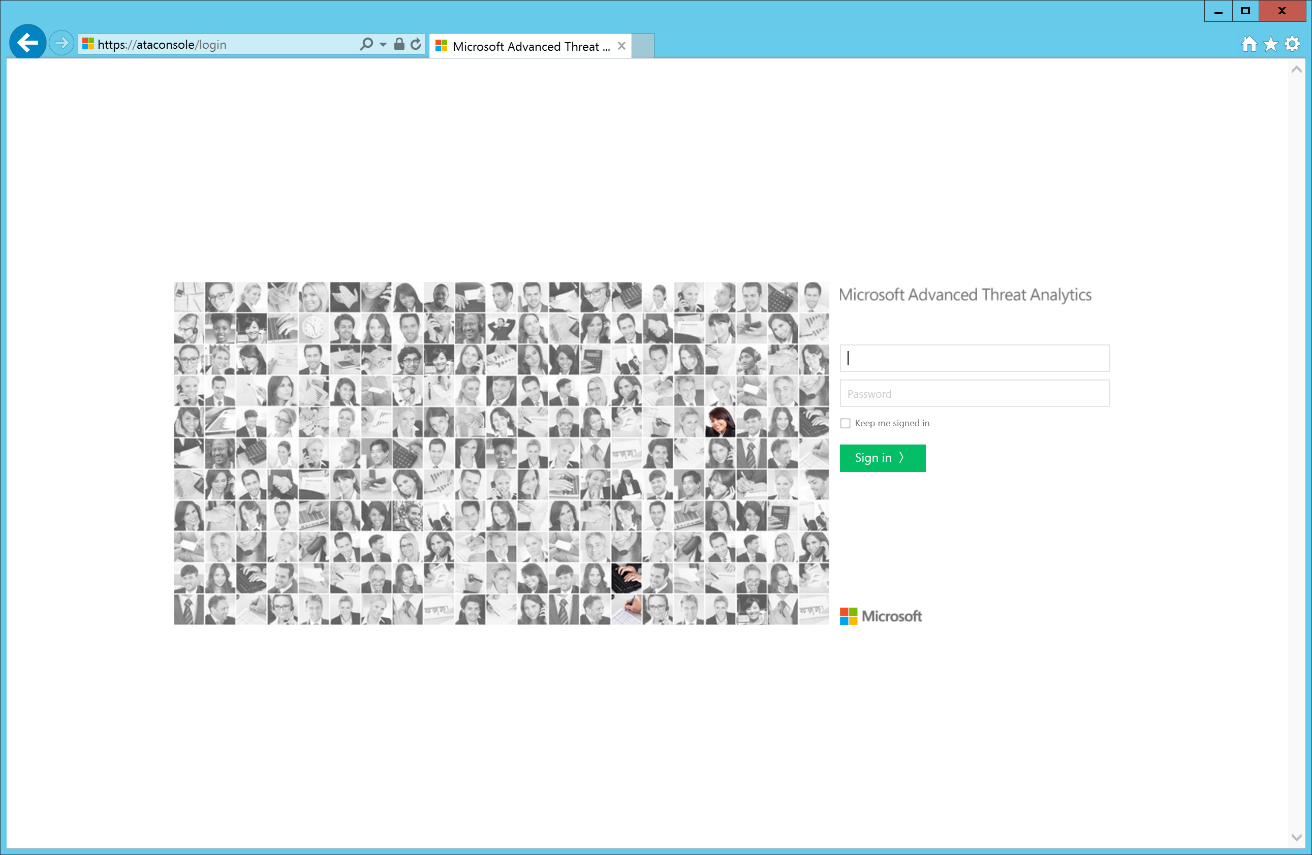
* 1. Inicio de sesión en la Consola

1. En el servidor del Centro ATA, haga clic en el icono de la **consola de Microsoft ATA** en el escritorio, o abra un explorador y navegue a la Consola de ATA.

Como alternativa, el administrador puede abrir un navegador desde el Centro ATA o de la Puerta de enlace de ATA y navegar a la dirección IP que el administrador configuró en la instalación del Centro ATA para la Consola de ATA.

1. Escriba el nombre de usuario y contraseña, y haga clic en **Iniciar sesión**.

El administrador tiene que iniciar sesión con un usuario que sea miembro del grupo de administradores locales o del grupo de administradores de Microsoft Advanced Threat Analytics.



* 1. Elementos de la consola

Una vez que se haya autenticado en la Consola de ATA, podrá ver los siguientes elementos.

Tabla 3: Elementos de la consola

| Elemento | Detalles |
| --- | --- |
| Escala de tiempo de ataques | Esta es la página predeterminada a la que será dirigido cuando el administrador inicie sesión en la Consola de ATA. De manera predeterminada, todas las actividades sospechosas se muestran en la escala de tiempo de ataques. El administrador puede filtrar la escala de tiempo de ataques para mostrar las actividades sospechosas en los siguientes estados: Todas, Abiertas, Descartadas o Resueltas. Las actividades sospechosas se listan por orden cronológico; las entradas más recientes se muestran primero en la lista. |
| Actividad sospechosa | Cuando ATA detecta una actividad sospechosa, se crea una entrada en la escala de tiempo de ataques. |
| Barra de notificaciones | Al detectar una nueva actividad sospechosa, la barra de notificación se abrirá automáticamente del lado derecho. Si hay nuevas actividades sospechosas desde la última vez que el administrador inició sesión, la barra de notificación se abrirá una vez que el administrador haya iniciado sesión correctamente. Para acceder a ella, el administrador puede hacer clic en la flecha de la derecha en cualquier momento. |
| Filtro | El administrador puede filtrar qué actividades sospechosas mostrar en la escala de tiempo de ataques o en la pestaña de actividades sospechosas del perfil de entidad, según el estado y la severidad. |
| Barra de búsqueda | En la parte superior de la pantalla, el administrador encontrará una barra de búsqueda. El administrador puede buscar un usuario, una computadora o grupos específicos en ATA. |
| Centro de mantenimiento[[1]](#footnote-2) | El Centro de mantenimiento proporciona alertas al administrador cuando algo no está funcionando correctamente en la red de ATA.  Cada vez que el sistema encuentre un problema, como un error de conectividad o una puerta de enlace de ATA desconectada, el icono Centro de mantenimiento se lo notificará al administrador, mostrando un punto rojo. |
| Configuración | Para modificar y ver la configuración de ATA; haga clic en el icono de configuración (tres puntos) en la barra de menús y luego haga clic en **Configuración**. |
| Perfiles de usuario y computadora | ATA crea un perfil para cada usuario y computadora en el dominio. En el perfil de usuario, ATA mostrará información general sobre el usuario y proveerá información adicional en las siguientes páginas: Resumen, Actividades y Actividades sospechosas. |
| Miniperfiles | En cualquier parte de la consola en donde se presente una sola entidad, como un usuario o computadora, si el administrador coloca el mouse sobre la entidad, se abrirá automáticamente un miniperfil. El perfil lista lo siguiente:   * Nombres * Imagen * Correo electrónico * Teléfono * Número de actividades sospechosas según la severidad |

1. Modificación de la configuración del Centro ATA

Tras la implementación inicial, las modificaciones al Centro ATA se deben realizar con cuidado. Siga las instrucciones a continuación cuando actualice la dirección IP y el puerto del certificado.

* 1. Modificación de la dirección IP

Las puertas de enlace de ATA almacenan localmente la dirección IP del Centro ATA al que deben conectarse. De forma periódica, se conectan al Centro ATA y descargan los cambios de configuración. El proceso de cambiar la forma en que las puertas de enlace de ATA se conectan al Centro ATA se lleva a cabo en dos fases.

Tabla 4: Fases de modificación de dirección IP—Centro

|  |  |
| --- | --- |
| Fase | Detalles |
| Primera | Actualice la dirección IP y el puerto que el administrador desea que utilice el servicio del Centro ATA.  En esta etapa, el Centro ATA todavía escucha en la dirección IP original. La próxima vez que la puerta de enlace de ATA sincronice su configuración, tendrá dos direcciones IP para el Centro ATA.  Siempre que la puerta de enlace de ATA pueda conectarse con la primera dirección IP, no intentará hacerlo con la nueva dirección IP y el nuevo puerto. |
| Segunda | Una vez que se hayan sincronizado todas las puertas de enlace de ATA con la configuración actualizada, active la nueva dirección IP y el puerto en el que escucha el Centro ATA. Cuando el administrador active la nueva dirección IP, el servicio del Centro ATA se vinculará a la nueva dirección IP.  Las puertas de enlace de ATA no podrán conectarse a la dirección original y ahora intentarán conectarse con la segunda dirección IP que tienen para el Centro ATA.  Después de conectarse con el Centro ATA en la nueva dirección IP, la puerta de enlace de ATA descargará la configuración más reciente y tendrá una sola dirección IP para el Centro ATA (a menos que el administrador inicie el proceso de nuevo). |

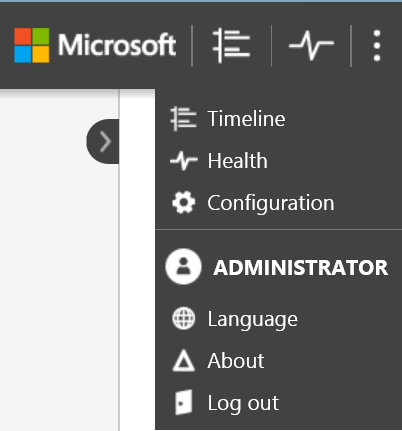
**Nota:** Si una puerta de enlace de ATA estaba desconectada durante la primera etapa y nunca recibió la configuración actualizada, el administrador tendrá que actualizar el archivo de Notación de Objetos de JavaScript (JSON) manualmente en la puerta de enlace de ATA.

Si la nueva dirección IP está instalada en el servidor del Centro ATA, el administrador puede seleccionarla de la lista de direcciones IP al realizar el cambio. Sin embargo, si por alguna razón el administrador no puede instalar la dirección IP en el servidor del Centro ATA, podrá optar por agregar manualmente una dirección IP personalizada. El administrador no podrá activar la dirección IP actualizada sino hasta que la dirección IP esté instalada en el servidor.

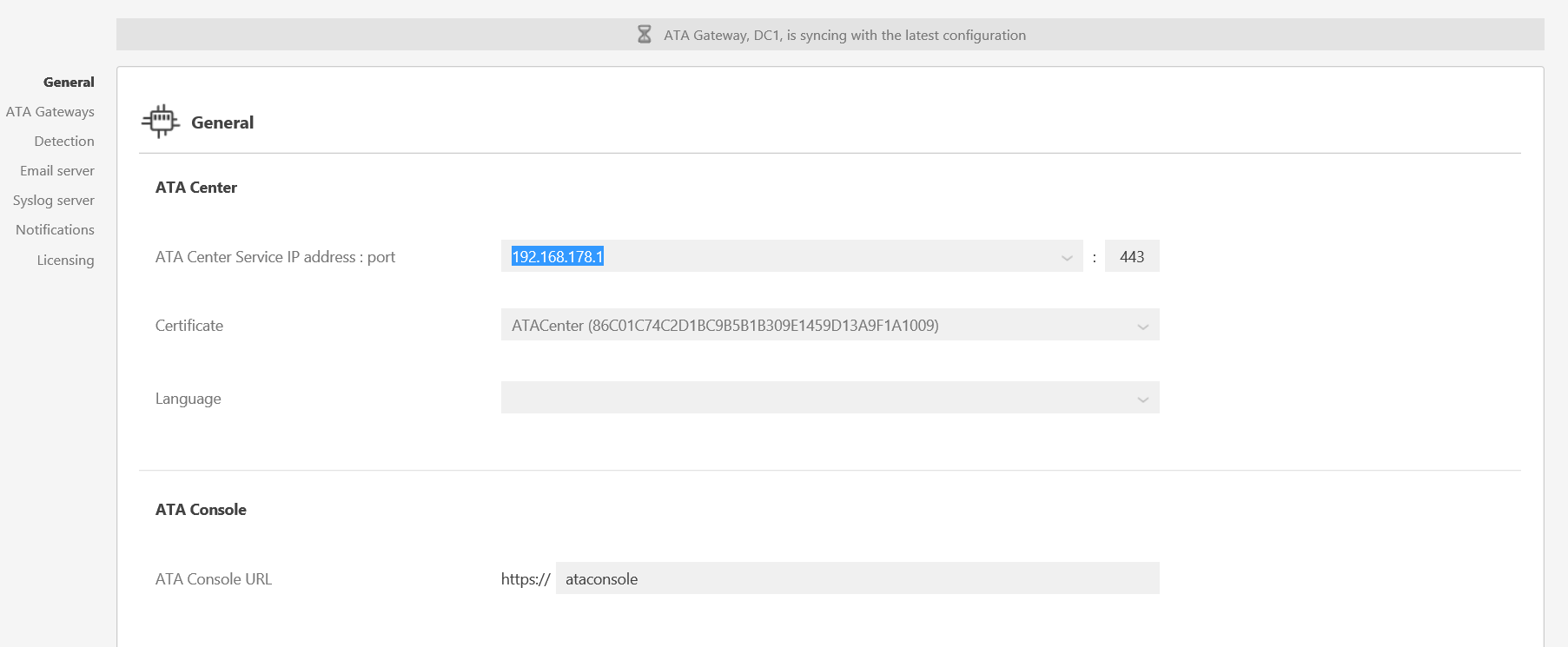
Si el administrador necesita implementar una nueva puerta de enlace de ATA después de activar la nueva dirección IP, tendrá que volver a descargar el paquete de configuración de puerta de enlace de ATA.

* + 1. Procedimiento para modificar la dirección IP

1. Abra la **Consola de ATA**.
2. En la barra de herramientas, haga clic en el icono de configuración  y luego en **Configuración**.



1. Haga clic en **General**.
2. En **Dirección IP del servicio del Centro ATA: puerto**, seleccione una de las direcciones IP existentes o haga clic en **Agregar dirección IP personalizada** y luego escriba una dirección IP.
3. Haga clic en **Guardar**.
4. El administrador verá una notificación de cuántas puertas de enlace de ATA se sincronizaron con la configuración más reciente.



1. Una vez que se hayan sincronizado todas las puertas de enlace de ATA, haga clic en **Activar** para activar la nueva dirección IP. Si el administrador introdujo una dirección IP personalizada, no podrá hacer clic en **Activar** hasta que haya instalado la dirección IP en el Centro ATA.
2. Una vez que se haya activado la nueva dirección IP, compruebe que todos las puertas de enlace de ATA puedan sincronizar sus configuraciones. La barra de notificaciones indicará cuántas puertas de enlace de ATA sincronizaron correctamente su configuración.
   1. Modificación del certificado

Si los certificados van a expirar y es necesario renovarlos o reemplazarlos después de instalar el nuevo certificado en el almacén de la computadora local en el servidor del Centro ATA, reemplace el certificado siguiendo este proceso de dos fases.

Tabla 5: Actualización del certificado—Centro ATA

|  |  |
| --- | --- |
| Fase | Detalles |
| Primera | Actualice el certificado que el administrador desea que utilice el servicio del Centro ATA. En esta etapa, el servicio del Centro ATA todavía estará enlazado al certificado original. Cuando las puertas de enlace de ATA sincronicen su configuración, tendrán dos certificados potenciales válidos para la autenticación mutua. Siempre que la puerta de enlace de ATA pueda conectarse con el certificado original, no intentará hacerlo con el nuevo. |
| Segunda | Después de que las puertas de enlace de ATA se hayan sincronizado con la configuración actualizada, el administrador podrá activar el nuevo certificado al que está enlazado el servicio del Centro ATA. Cuando el administrador active el nuevo certificado, el servicio del Centro ATA se enlazará con el certificado. Las puertas de enlace de ATA no podrán autenticar mutuamente el servicio del Centro ATA de manera correcta, por lo que intentarán autenticar el segundo certificado. Después de conectarse con el servicio del Centro ATA, la puerta de enlace de ATA descargará la configuración más reciente y tendrá un solo certificado para el Centro ATA (a menos que el administrador haya vuelto a iniciar el proceso). |

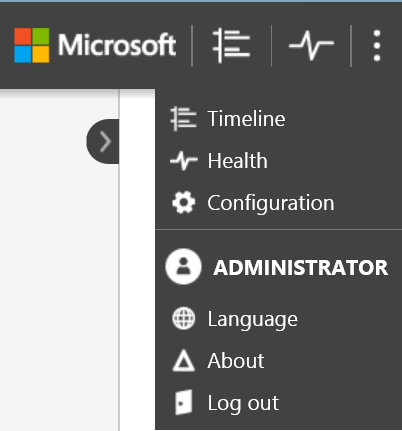
**Nota:** Si una puerta de enlace de ATA estaba desconectada durante la primera fase y nunca llegó a actualizar su configuración, el administrador tendrá que actualizar manualmente el archivo de configuración JSON en la puerta de enlace de ATA.

El certificado que use el administrador debe ser de confianza para las puertas de enlace de ATA.

Si el administrador necesita implementar una nueva puerta de enlace de ATA después de activar el nuevo certificado, tendrá que volver a descargar el paquete de configuración de puerta de enlace de ATA.

* + 1. Procedimiento para modificar el certificado

1. Abra la Consola de ATA.
2. En la barra de herramientas, haga clic en el icono de configuración  y luego en **Configuración**.



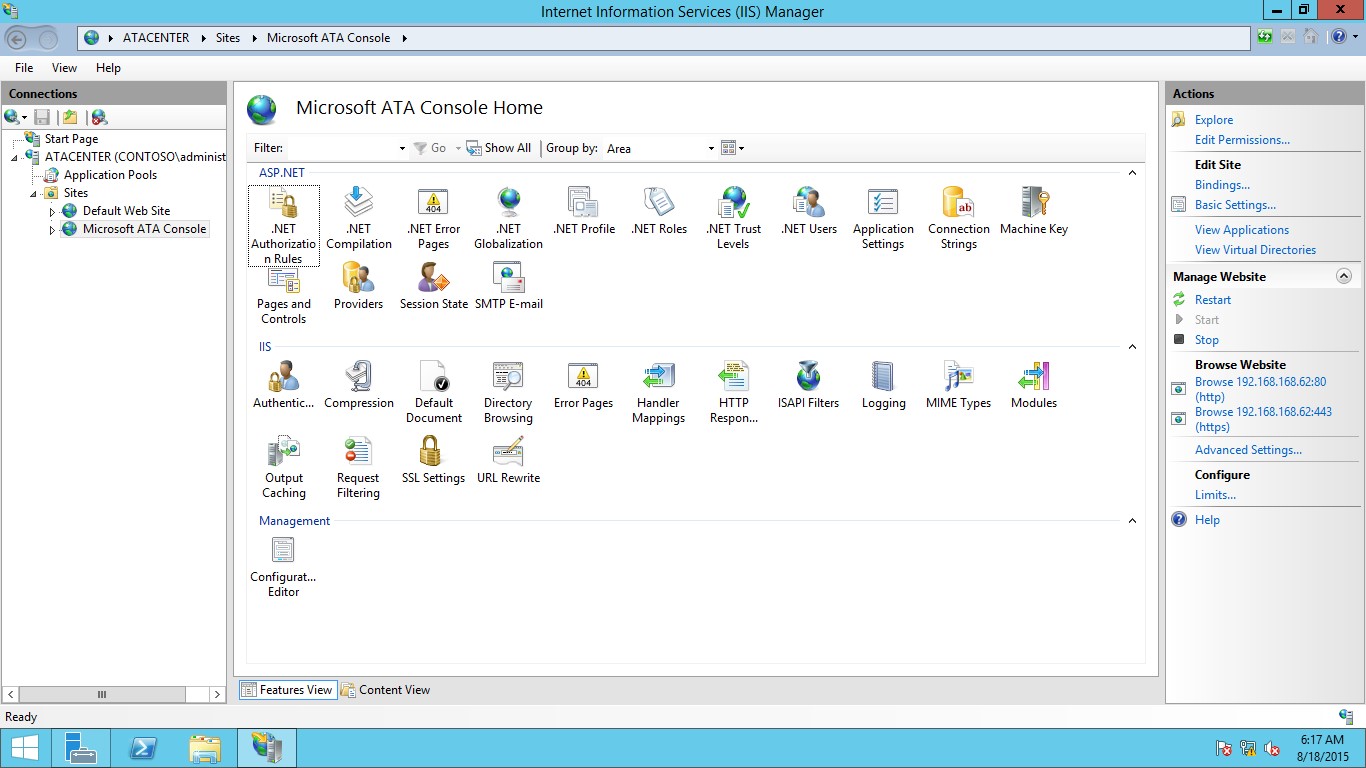
1. Haga clic en **General**.
2. En **Certificado**, seleccione uno de los certificados de la lista.
3. Haga clic en **Guardar**.
4. El administrador verá una notificación de cuántas puertas de enlace de ATA se sincronizaron con la configuración más reciente.
5. Una vez que se hayan sincronizado todos las puertas de enlace de ATA, haga clic en **Activar** para activar el nuevo certificado.
6. Compruebe que todas las puertas de enlace de ATA puedan sincronizar sus configuraciones una vez que se active el cambio.
   1. Modificación de la dirección IP de la consola

De manera predeterminada, la URL de la Consola de ATA es la dirección IP que se seleccionó para la dirección IP de la Consola de ATA cuando el administrador instaló el Centro ATA.

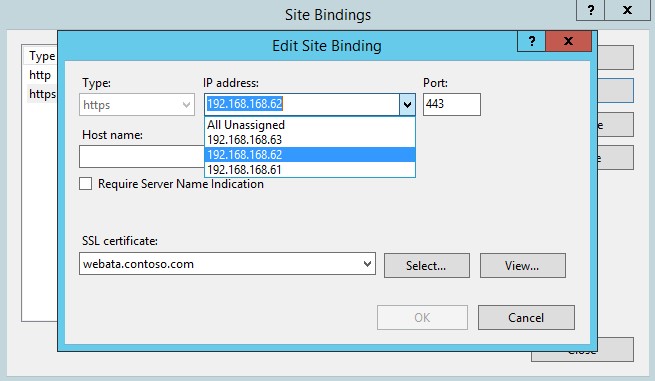
La URL se utiliza en los siguientes escenarios:

* **Instalación de puertas de enlace de ATA**: cuando se instala una puerta de enlace de ATA, se registra automáticamente en el Centro ATA. El proceso de registro se realiza a través de la conexión con la Consola de ATA.. Si el administrador introduce un nombre de dominio completo (FQDN) para la dirección URL de la Consola de ATA, el administrador necesita validar que la puerta de enlace pueda resolver el FQDN en la dirección IP con la que está enlazada la Consola de ATA en el Administrador de Internet Information Services (IIS). Adicionalmente, la URL se usa para crear el acceso directo a la Consola de ATA en las puertas de enlace de ATA.
* **Alertas**: cuando ATA envía una alerta por email o SIEM, incluye un vínculo a la actividad sospechosa. La parte del vínculo correspondiente al host es la configuración de URL de la Consola de ATA.
* Si el administrador instaló un certificado de la entidad de certificación interna, probablemente quiera que la URL coincida con el nombre del firmante del certificado, para que los usuarios no reciban un mensaje de advertencia al conectarse a la Consola de ATA.
* El uso de un FQDN para la dirección URL de la Consola de ATA, permite al administrador modificar la dirección IP que utiliza IIS para la Consola de ATA sin interrumpir las alertas que se enviaron en el pasado o sin tener que volver a descargar el paquete de puesta de enlace de ATA. El administrador solamente tendrá que actualizar el sistema de nombres de dominio (DNS) con la nueva dirección IP.
  + 1. Procedimiento para modificar la dirección IP de la consola

1. Instale la dirección IP en el servidor del Centro ATA.
2. Abra el Administrador de IIS.
3. Expanda el nombre del servidor y expanda **Sitios**.
4. Seleccione el sitio de la Consola de Microsoft ATA.
5. En el panel **Acciones**, en la sección **Editar sitio**, haga clic en **Enlaces**.



1. Haga clic en **http** y luego en **Editar** para seleccionar la nueva dirección IP. Haga lo mismo para **https,** seleccionando la misma dirección IP.



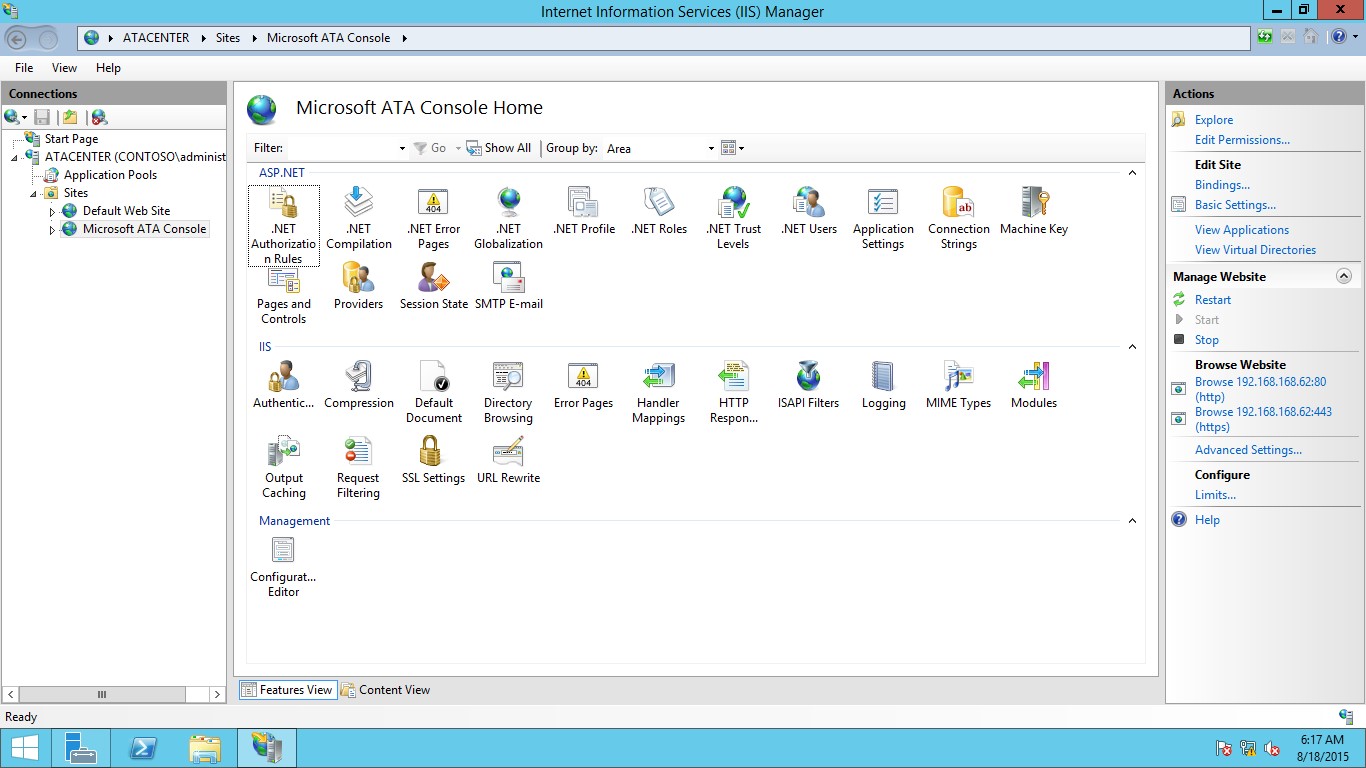
1. En el panel **Acción**, en la sección **Administrar sitio web**, haga clic en **Reiniciar**.
2. Vaya al símbolo de sistema como administrador y escriba los siguientes comandos para actualizar la dirección HTTP. sys driver:
   1. Para agregar la nueva dirección IP: **netsh http add iplisten ipaddress=nuevadirecciónip**
   2. Para ver si se está usando la nueva dirección: **netsh http show iplisten**
   3. Para eliminar la dirección IP anterior: **netsh http delete iplisten ipaddress=direcciónipanterior**
3. Si la dirección URL de la Consola de ATA sigue usando una dirección IP, actualice la URL de la Consola de ATA con la nueva dirección IP y descargue el paquete de configuración de puerta de enlace de ATA antes de implementar nuevas puertas de enlace de ATA.
4. Si la dirección URL de la Consola de ATA es un FQDN, actualice el DNS con la nueva dirección IP para el FQDN.
   1. Modificación del certificado de IIS

En la consola, el administrador puede seleccionar y modificar el certificado para el servicio del Centro ATA, pero no puede cambiar el certificado que utiliza IIS. Si el administrador necesita modificar el certificado que utiliza IIS para el Centro ATA, siga estos pasos desde el servidor del Centro ATA.

**Nota:** Después de modificar el certificado de IIS, el administrador debe descargar el paquete de configuración de puertas de enlace de ATA antes de instalar nuevas puertas de enlace de ATA.

* + 1. Procedimiento para modificar el certificado de IIS

1. Instale el nuevo certificado en el servidor del Centro ATA.
2. Abra el Administrador de IIS.
3. Expanda el nombre del servidor y expanda **Sitios**.
4. Seleccione el sitio de la Consola de Microsoft ATA.
5. En el panel **Acciones**, en la sección **Editar sitio**, haga clic en **Enlaces**.

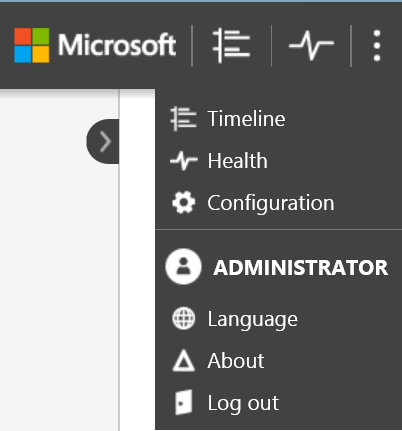


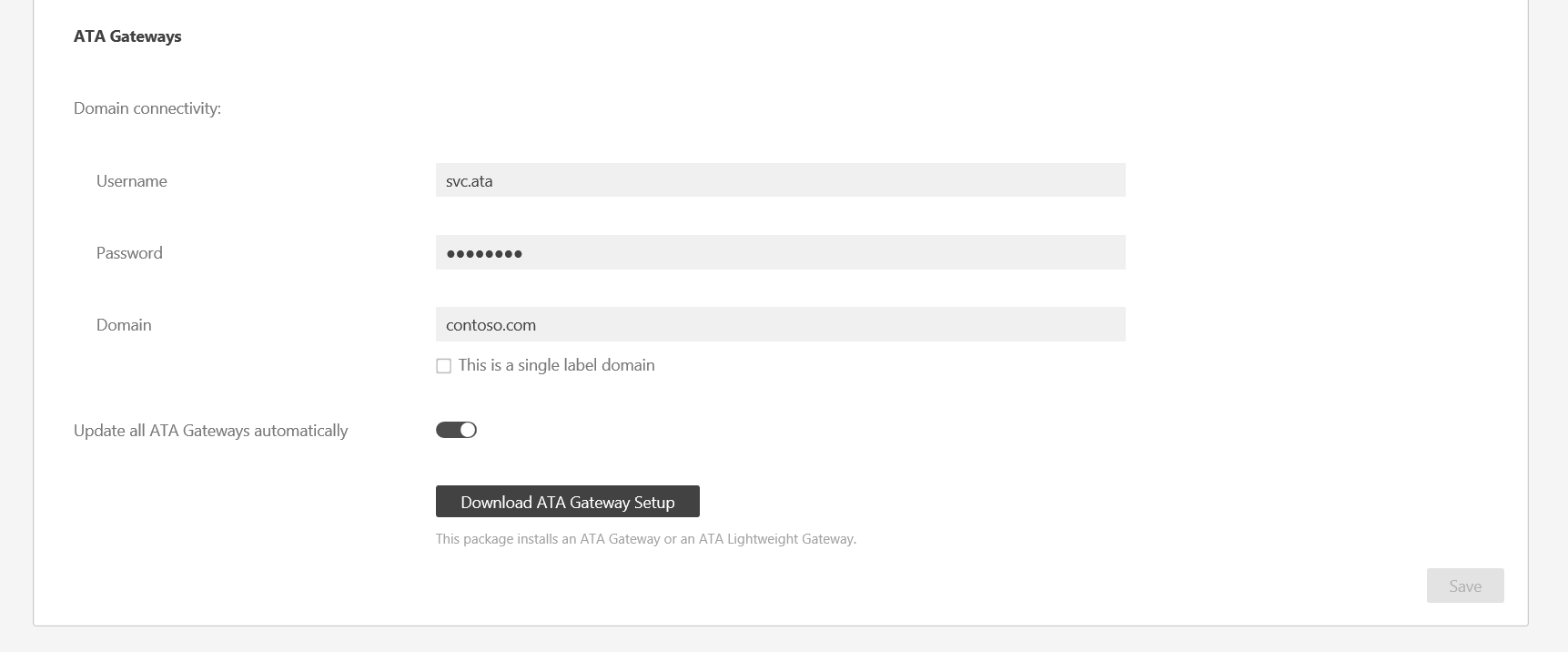
1. Haga clic en **https** y luego seleccione **Editar**.
2. En **Certificado SSL**, seleccione el nuevo certificado.
3. Descargue el paquete de configuración de puerta de enlace de ATA antes de instalar una nueva puerta de enlace de ATA.
4. Modificación de la configuración de la puerta de enlace de ATA
   1. Modificación de la contraseña de conectividad de dominio

Si el administrador modifica la contraseña de conectividad de dominio, asegúrese de que la contraseña que introduzca el administrador sea correcta. De lo contrario, el servicio de ATA dejará de ejecutarse en las puertas de enlace de ATA.

Si el administrador sospecha que esto es lo que ha ocurrido, en la puerta de enlace de ATA, busque lo siguiente en el archivo **Microsoft.Tri.Gateway-Errors.log**: The supplied credential is invalid. (La credencial suministrada es inválida).

* + 1. Procedimiento para modificar la contraseña de conectividad de dominio

1. Abra la Consola de ATA en la puerta de enlace de ATA.
2. En la barra de herramientas, haga clic en el icono de configuración  y luego en **Configuración**.
3. Haga clic en **General**.



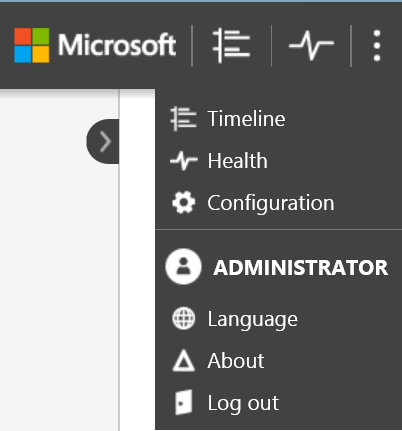
1. En **Puertas de enlace de ATA**, cambie la contraseña.
2. Haga clic en **Guardar**.
3. Después de cambiar la contraseña, compruebe manualmente que el servicio de puerta de enlace de ATA se está ejecutando en los servidores de puerta de enlace de ATA.
4. Alertas de ATA

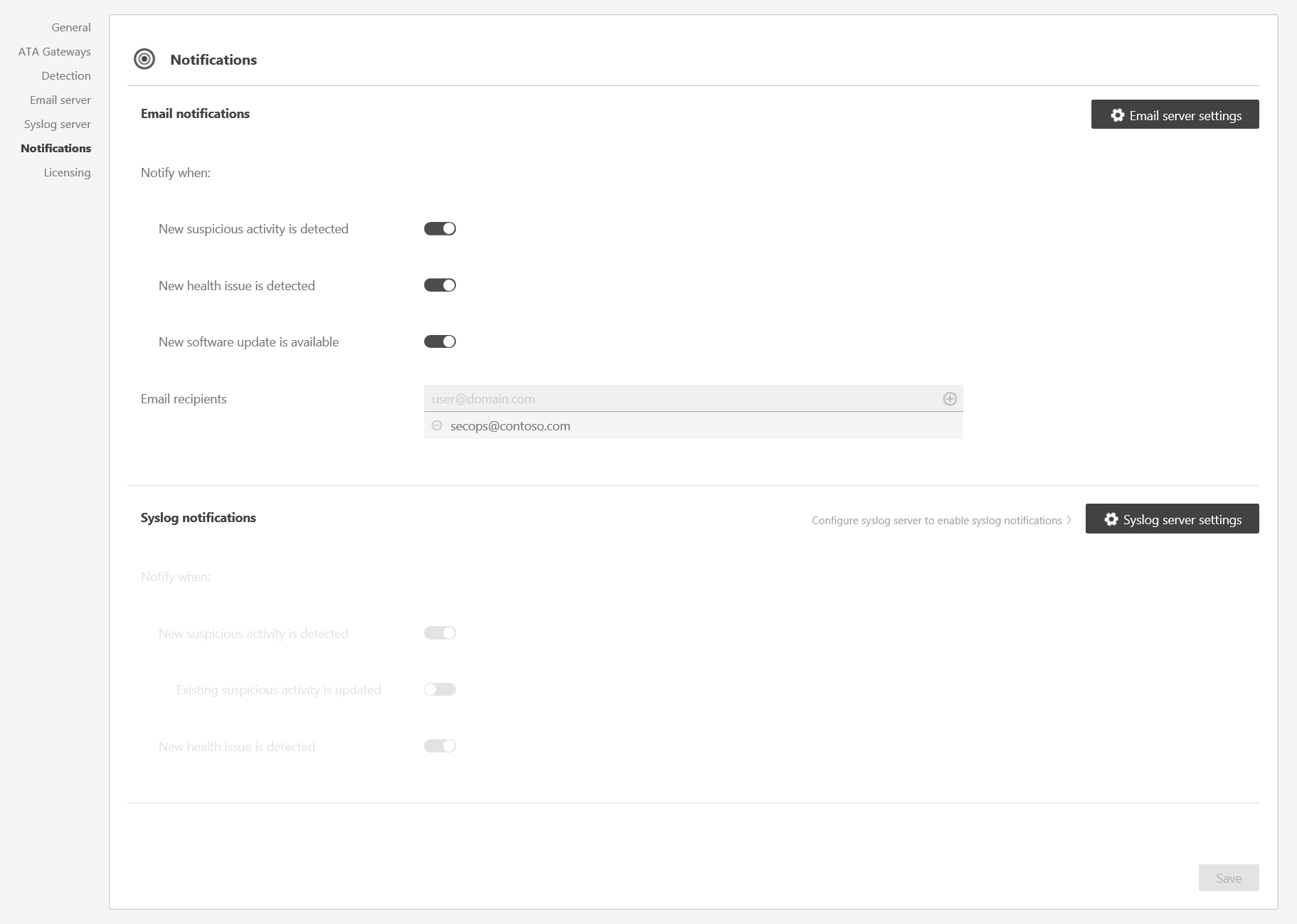
Cuando ATA detecta una actividad sospechosa, puede alertar al administrador ya sea por correo electrónico o enviando la alerta al servidor Syslog. Si el administrador implementa uno de estos tipos de alerta o ambos, puede configurar lo siguiente para las alertas.

**Nota:** Las notificaciones incluirán un vínculo que lleve directamente al usuario a la actividad sospechosa detectada. La parte del vínculo correspondiente al nombre de host se toma de la configuración de la dirección URL de la Consola de ATA en la página del Centro ATA. De manera predeterminada, la URL de la Consola de ATA es la dirección IP seleccionada durante la instalación del Centro ATA. Si el administrador va a configurar alertas por correo electrónico o Syslog, recomendamos usar un FQDN como la dirección URL de la Consola de ATA.

Las alertas de estado del sistema se envían solamente por correo electrónico.

* 1. Configuración de idioma y nivel de detalle de alerta (breve o detallada)

1. Abra la consola del Centro ATA.
2. En la barra de herramientas, haga clic en el icono de configuración  y luego en **Configuración**.
3. Haga clic en **Notificaciones**.
4. En **Notificar cuando**, deslice los controles a la derecha para las notificaciones que desee habilitar.



1. Haga clic en **Guardar**.
   1. Configuración de alertas por correo electrónico

ATA puede alertar al administrador cuando detecte una actividad sospechosa. Si el administrador implementa las alertas por correo electrónico, puede configurar lo siguiente para éstas.

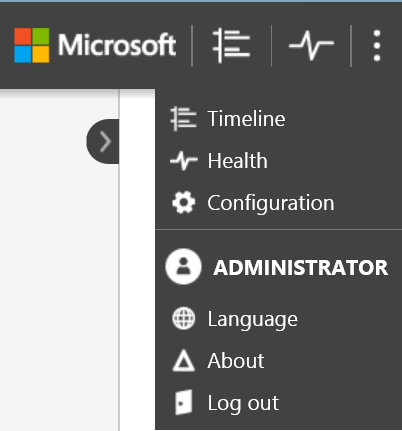
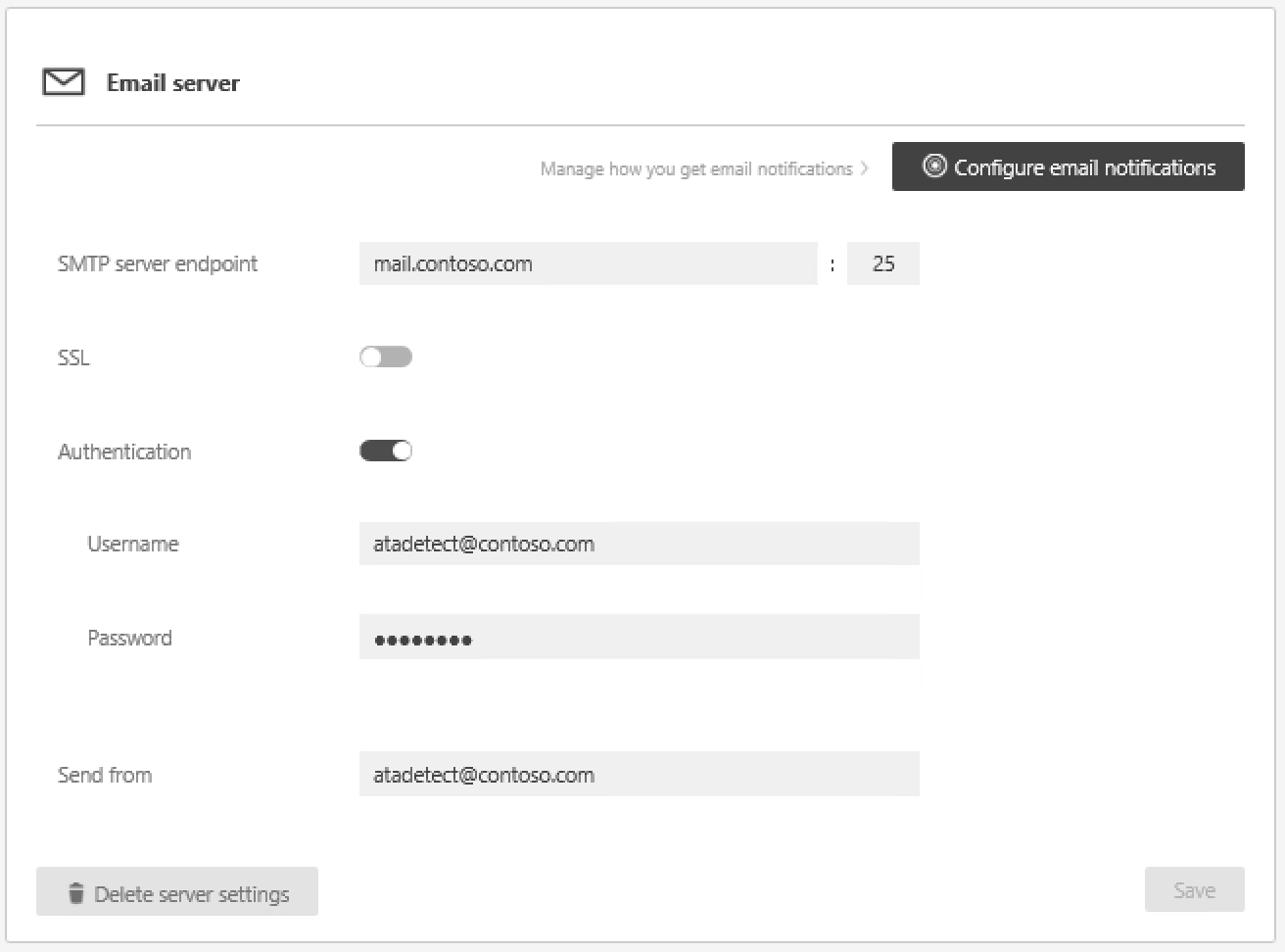
1. Abra la consola del Centro ATA.
2. En la barra de herramientas, haga clic en el icono de configuración  y luego en **Configuración**.
3. Haga clic en **Servidor de correo electrónico**.
4. Ingrese la siguiente información:

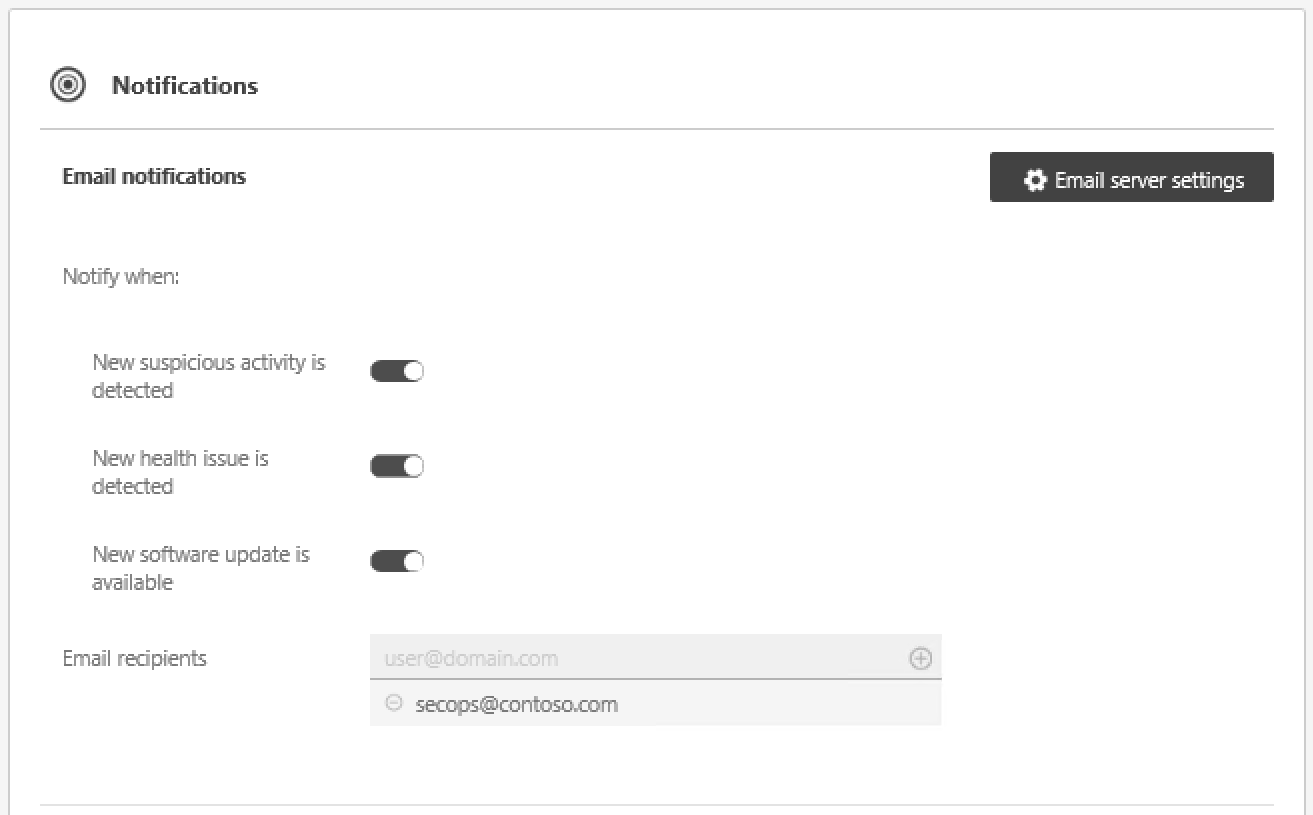
Tabla 6: Configuración de alertas por correo electrónico

| Campo | Descripción | Valor |
| --- | --- | --- |
| Extremo de servidor SMTP (requerido) | Introduzca el FQDN del servidor SMTP. | Por ejemplo: smtp.contoso.com |
| SSL | Activar la Capa de sockets seguros (SSL) si el servidor SMTP requiere SSL.   |  | | --- | | **System_CAPS_noteNota** | | Si el administrador implementa SSL, BCI también tendrá que cambiar el número de puerto. | | Desactivado por defecto |
| Autenticación | Implementar si el servidor SMTP requiere autenticación.   |  | | --- | | **System_CAPS_noteNota** | | Si BCI implementa autenticación, el administrador debe proporcionar un nombre de usuario y contraseña para una cuenta de correo electrónico que tenga permiso para conectarse con el servidor SMTP. | | Desactivado por defecto |
| Enviar desde (requerido) | Introduzca una dirección de correo electrónico desde la que se enviará el correo electrónico. | Por ejemplo: ATA@contoso.com |



Una vez que se complete la configuración de correo electrónico, haga clic en **Configurar notificaciones de correo electrónico**. Hay 3 tipos de notificaciones que pueden activarse/desactivarse:

* Se ha detectado nueva actividad sospechosa
* Se ha detectado nuevo problema de mantenimiento
* Hay una nueva actualización de software disponible



Después de activar los tipos de notificación deseados y de especificar los destinatarios que recibirán las notificaciones, haga clic en Guardar en la parte inferior de la página.

* 1. Configurar alertas Syslog (informativas)

La configuración de Syslog está fuera del alcance de este proyecto. Esta sección es informativa para que BCI pueda configurar el reenvío a Syslog.

ATA puede alertar a BCI cuando detecte una actividad sospechosa, enviando la alerta al servidor de Syslog. ATA puede recibir también eventos Syslog de proveedores selectos. Vea la lista de proveedores en <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/configure-event-collection> (Configurar recopilación de eventos).

Vea también <https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/setting-ata-alerts> para trabajar con alertas y configurar ATA para enviar datos a un servidor Syslog.

BCI debe trabajar con la documentación e instrucciones que ofrece el proveedor del servicio Syslog o SIEM en conjunto con la guía que se ofrece en esta sección.

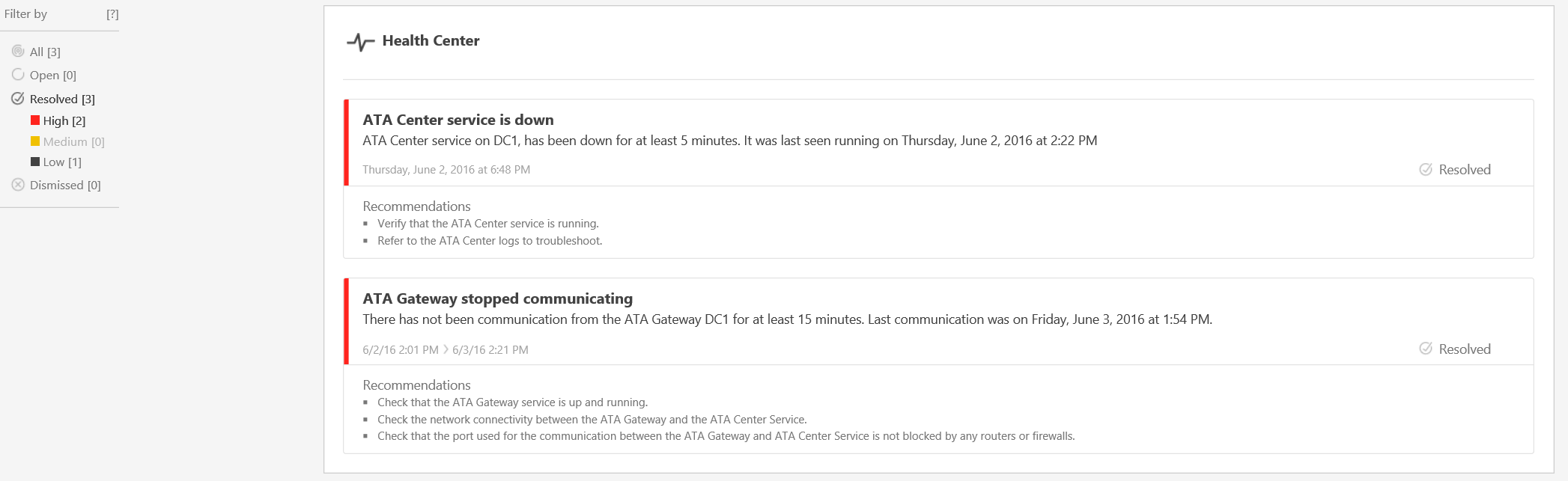
1. Centro de mantenimiento de ATA

El Centro de mantenimiento de ATA notifica a BCI sobre un problema generando una alerta (un punto rojo) sobre el icono Centro de mantenimiento en la barra de menús.

* 1. Administración de estado y alertas de ATA

ATA red dotPara comprobar el estado general del sistema, haga clic en el icono **Centro de mantenimiento** en la barra de menús.

* Las alertas abiertas se pueden administrar definiéndolas como **Resueltas** o **Descartadas**. En la alerta, haga clic en **Abrir** y luego desplácese hasta **Resuelta** o **Descartada**.
* Si el administrador resuelve un problema y ATA detecta que éste persiste, el problema regresará a la lista de problemas **abiertos**. Si ATA detecta que se resolvió un problema abierto, lo moverá automáticamente a la lista de problemas **resueltos**.
* **La lista de problemas descartados** incluye aquellos que el administrador no desea que ATA siga comprobando; por ejemplo, si recibe alertas de un problema que sabe que existe, que no planea resolver, y del cual no desea seguir recibiendo notificaciones ni verlo en la lista de problemas **abiertos**, el administrador puede establecerlo como **descartado**.



1. Actividades sospechosas

Esta sección explica cómo trabajar con actividades sospechosas. No cubre cómo responder a las actividades sospechosas, sino más bien cómo trabajar con ellas en la consola, agregar comentarios y filtrar estas actividades.

* 1. Revisar actividades sospechosas en la escala de tiempo de ataques

Después de iniciar sesión en la Consola de ATA, se muestra automáticamente al administrador la **Escala de tiempo de actividades sospechosas** abierto. Las actividades sospechosas se muestran en orden cronológico con las actividades sospechosas más recientes en la parte superior de la escala de tiempo. Cada actividad sospechosa tiene la siguiente información:

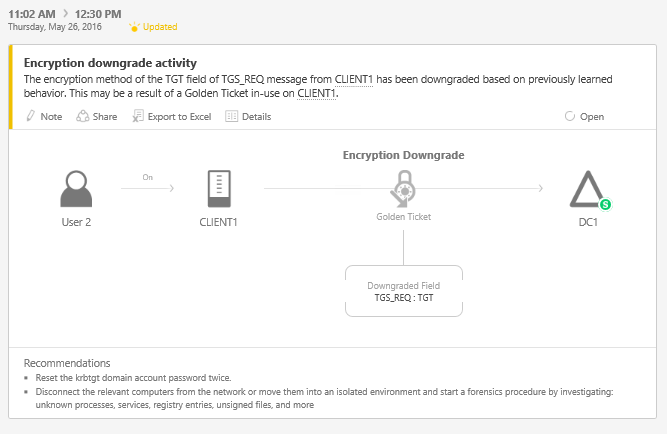
* Entidades involucradas, incluyendo usuarios, computadoras, servidores, controladores de dominio y recursos
* Horas y periodo de tiempo de las actividades sospechosas
* Gravedad de la actividad sospechosa: alta, media o baja.
* Estado: abierta, resuelta o desechada

La escala de tiempo de ataque también puede:

* Enviar la actividad sospechosa a otras personas en BCI por medio de correo electrónico. Para enviar estas notificaciones se requiere instalar un cliente de correo electrónico en la computadora en la que el administrador vaya a explorar las notificaciones.
* Exporte la actividad sospechosa a Excel.
* Agregue una nota a la actividad sospechosa.
* Proporcione información sobre la actividad sospechosa.

**Nota:** Si el administrador mueve el puntero del mouse sobre un usuario o computadora, se mostrará un miniperfil de entidad que proporciona información adicional sobre la entidad e incluye el número de actividades sospechosas vinculadas a esa entidad.

Si el administrador hace clic en una entidad, podrá ver el perfil de entidad del usuario o computadora.



**Advertencia:** La consola de amenazas ofrece recomendaciones acerca de cómo responder a la actividad sospechosa. Esta asesoría de alto nivel requiere de un plan de respuesta eficaz como parte de este proyecto (vea ATAIS: plan de respuesta). Cada actividad requiere de procesos exclusivos de atención y respuesta, dependiendo de la gravedad y el estado.

* 1. Filtrado de la lista de actividades

Para filtrar la lista de actividades sospechosas:

1. En el panel **Filtrar por** del lado izquierdo de la pantalla, haga clic en una de las siguientes opciones: **Todas**, **Abiertas**, **Resueltas** o **Descartadas**.
2. Para filtrar la lista aún más, haga clic en **Alta**, **Media** o **Baja**.
   * 1. Gravedad y estado de actividad sospechosa

La siguiente tabla describe la gravedad bajo la cual puede clasificarse cada actividad sospechosa.

Tabla 7: Gravedad de actividades sospechosas

| Nivel de gravedad | Descripción |
| --- | --- |
| BAJA | Indica actividades sospechosas que incluyen ataques individuales de usuarios maliciosos o por medio de software que puede usarse para obtener acceso a los datos de la organización. |
| MEDIA | Indica actividades sospechosas que pueden poner en riesgo a ciertas identidades específicas por ataques más graves que podrían resultar en robo de identidad o escalación de privilegios. |
| ALTA | Indica actividades sospechosas que pueden derivar en robo de identidad, escalación de privilegios u otros ataques de alto impacto. |

La siguiente tabla muestra el estado actual de la actividad que el administrador de ATA actualiza y modifica.

Tabla 8: Estado de las actividades sospechosas

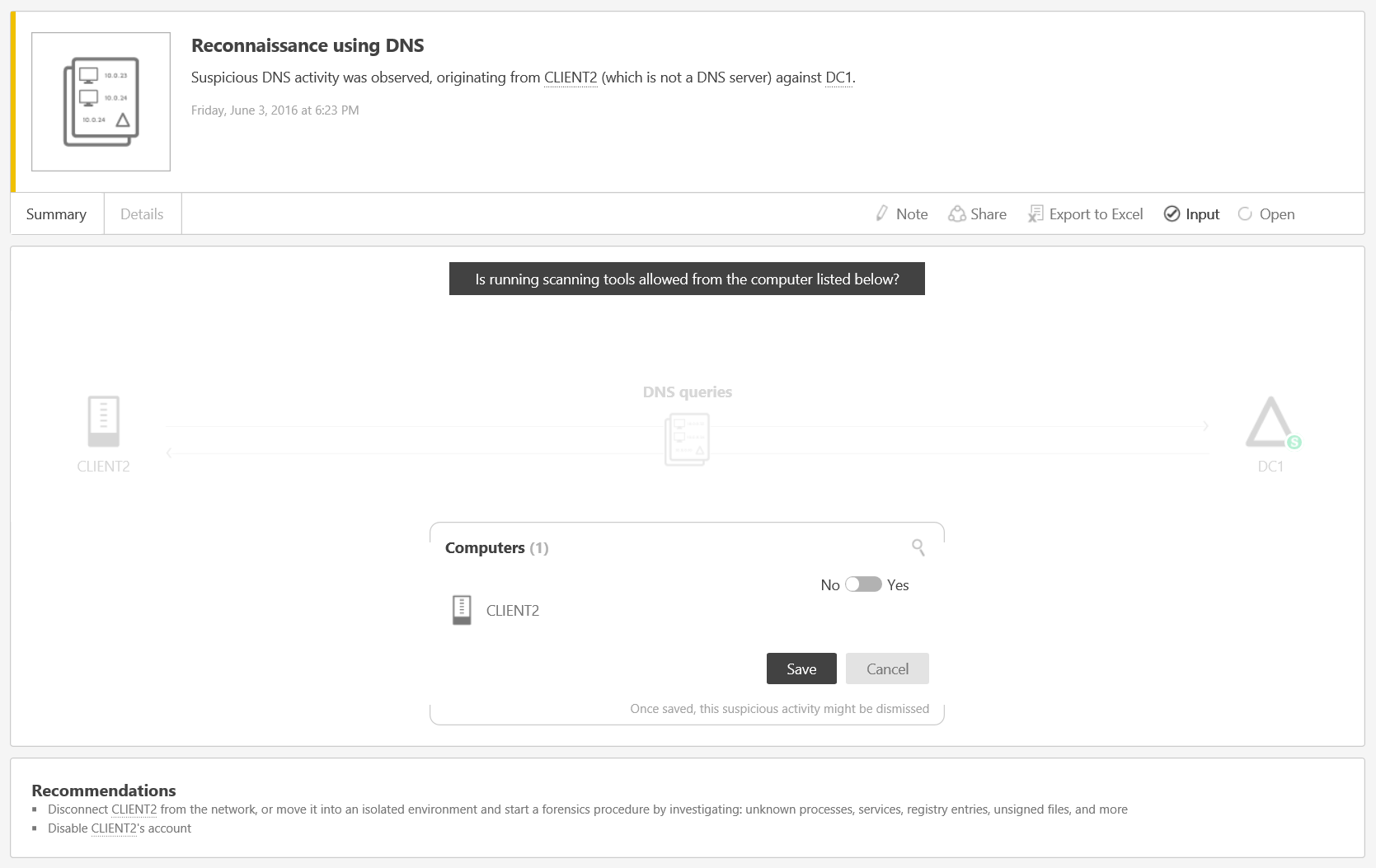
|  |  |
| --- | --- |
| Estado | Descripción |
| Abiertas | Todas las nuevas actividades sospechosas aparecen en esta lista. |
| Resueltas | Sirve para llevar un seguimiento de las actividades sospechosas que BCI identificó, investigó y corrigió o mitigó. |
| Descartadas | Actividades que BCI descartó en forma manual. Si ATA detecta una actividad sospechosa similar, se creará una nueva detección. |

**Nota:** ATA puede reabrir una actividad resuelta si esta misma actividad se detecta de nuevo en un periodo de tiempo corto.

* 1. Actualización de una actividad sospechosa

Para permitir que ATA aprenda sobre la red de BCI, algunas actividades sospechosas (reconocimiento de DNS, pass-the-ticket, comportamiento anormal y ejecución remota) solicitan información para mejorar la detección de actividades sospechosas.

1. Para las actividades sospechosas que permiten a BCI proporcionar información, la pregunta introducida se abre automáticamente. BCI deberá responder preguntas sobre las actividades en su red y si deberían considerarse sospechosas. En el siguiente ejemplo, se pregunta al administrador si se permite ejecutar herramientas de exploración en una computadora específica.



1. Si el administrador responde **No**, esta actividad se considerara sospechosa y cada vez que ATA encuentre esta actividad desde esta computadora, alertará a BCI.
2. No obstante, si el administrador responde **Sí**, la actividad sospechosa podría desecharse y las futuras actividades de este tipo provenientes de esta computadora tal vez no generen una actividad sospechosa o generen una actividad que se deseche automáticamente.
3. Si el administrador de ATA de BCI no está seguro, haga clic en **Cancelar** y luego consulte al responsable de la entidad.
4. BCI puede cambiar el estado de una actividad sospechosa haciendo clic en el estado actual de la actividad sospechosa y seleccionando una de las siguientes opciones: **Abierta**, **Resuelta** o **Descartada**.
5. Configuración de detección de ATA

En la página de configuración de Detección, BCI puede crear una lista de direcciones IP y subredes que tengan circunstancias inusuales y deban manejarse de una forma ligeramente distinta a otras entidades en la red.

En la página **Detección** el administrador puede definir los elementos en la siguiente tabla.

Tabla 9: Opciones de configuración de detección

|  |  |
| --- | --- |
| Elemento | Descripción |
| Subredes de arrendamiento a corto plazo | Si BCI tiene subredes en las que las direcciones IP sean de corto plazo, como subredes con direcciones IP de red privada virtual o subredes WiFi, es importante introducir estas direcciones IP y subredes en ATA para que almacene la asociación entre una computadora y una dirección IP de estos rangos por un periodo más corto de tiempo que para otras direcciones IP. |
| Identificadores de seguridad de cuenta (SID) de honeytoken | Esta es una cuenta de usuario que no debería tener actividades de red. Esta cuenta se configurará como el usuario de honeytoken de ATA. Si alguien intenta usar esta cuenta de usuario, ATA creará una actividad sospechosa y la marcará como indicación de una actividad malintencionada. Para configurar el usuario de honeytoken, el administrador necesitará el SID de la cuenta de usuario, no el nombre de usuario.  Para encontrar el SID de un usuario, ejecute el siguiente cmdlet de Windows PowerShell: **Get-ADUser NombreUsuario -Propiedades**. |
| Exclusiones de detección | BCI puede excluir direcciones IP de las siguientes detecciones. Si BCI introduce una dirección IP en una de estas listas, ATA la excluirá de este tipo específico de actividad detectada.   * Exclusiones de dirección IP de reconocimiento de DNS * Exclusiones de dirección de IP por pass-the-ticket |

1. Base de datos de ATA

ATA usa una base de datos de código fuente abierto con los acuerdos relevantes implementados como parte de la instalación de ATA. Esta base de datos se conoce como MongoDB. La versión más reciente de ATA usa *wiredtiger* en vez del motor de almacenamiento mmapv1 anterior.

Las siguientes fuentes y procedimientos ayudarán a BCI a hacer copias de seguridad, mover y administrar la base de datos, de ser necesario.

* 1. Copia de seguridad de la base de datos

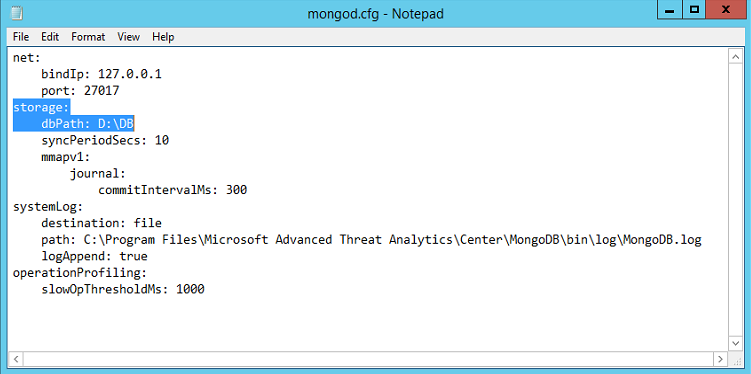
Consulte la [documentación pertinente de MongoDB](http://docs.mongodb.org/manual/administration/backup/).

* 1. Restauración de la base de datos

Consulte la [documentación pertinente de MongoDB](http://docs.mongodb.org/manual/administration/backup/).

* 1. Mover la base de datos

1. Detenga el servicio **Microsoft Advanced Threat Analytics Center**.
2. Detenga el servicio **MongoDB**.
3. Abra el archivo de configuración de Mongo, que se encuentra de forma predeterminada en: C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\mongod.cfg.
4. Busque el parámetro *storage: dbPath*.
5. Mueva la carpeta que aparece en el parámetro *dbPath* a la nueva ubicación.
6. Cambie el parámetro *dbPath* del archivo de configuración de Mongo por la nueva ruta de acceso de carpeta; después guarde y cierre el archivo.



1. Inicie el servicio **MongoDB**.
2. Abra una ventana de símbolo del sistema y ejecute el shell de Mongo mediante el siguiente comando: **mongo.exe ATA**.

Por defecto, el archivo mongo.exe se encuentra en: C:\Program Files\Microsoft Advanced Threat Analytics\Center\MongoDB\bin

1. Ejecute el siguiente comando:

**db.SystemProfiles.update( {\_t: "CenterSystemProfile"} , {$set:{"Configuration.CenterDatabaseClientConfiguration.DataPath" : "<*Nueva ubicación de bD*>"}})** en donde <*Nueva ubicación de bD*> es la nueva ruta de acceso de carpeta.

1. Inicie el servicio **Microsoft Advanced Threat Analytics Center** .
   1. Administración de la base de datos

Consulte la [documentación pertinente de Robomongo](https://robomongo.org/). ***Microsoft no admite la modificación de la base de datos de ATA***.

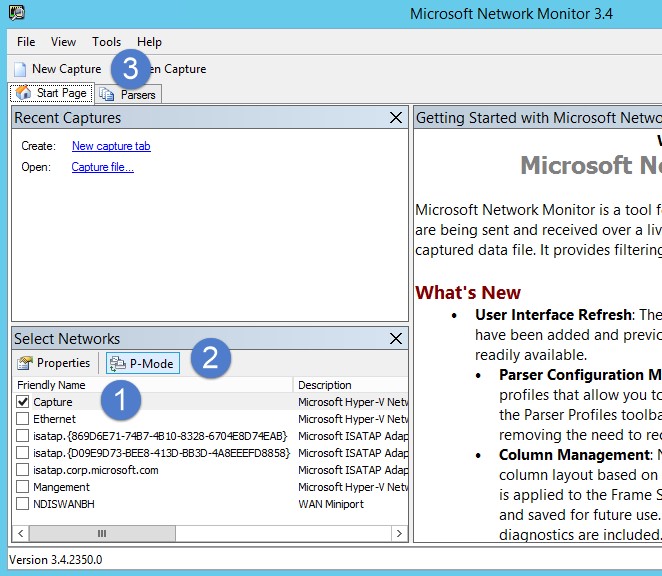
1. Validación de creación de reflejo del puerto

Los siguientes pasos guiarán al administrador a través del proceso para validar que la creación de reflejo del puerto esté correctamente configurada y que funcione correctamente si se usó Creación de reflejo de puerto en vez de puerta de enlace ligera de ATA.

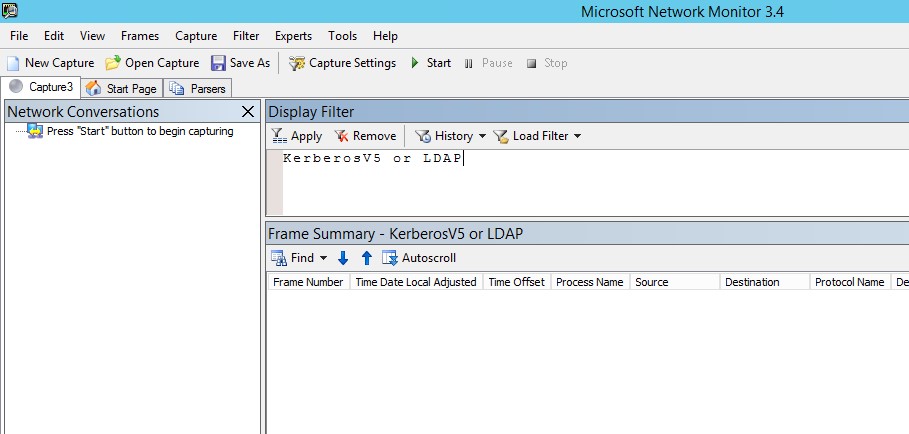
Instale [Microsoft Network Monitor 3.4](https://www.microsoft.com/download/details.aspx?id=4865) u otra herramienta de examen de redes. No instale Microsoft Message Analyzer ni ningún otro software de captura de tráfico en la puerta de enlace de ATA.

Abra Network Monitor y cree una nueva pestaña de captura.

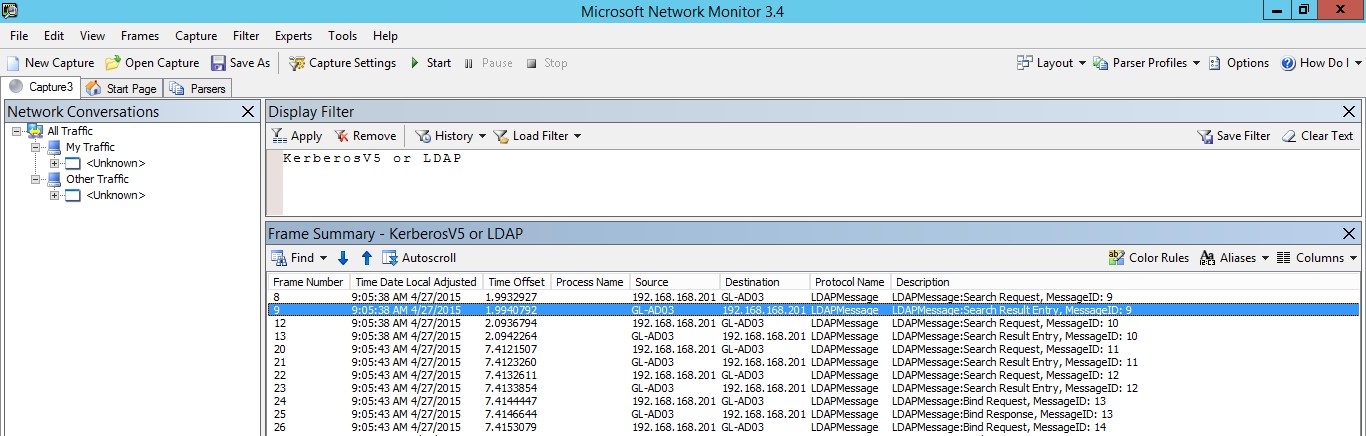
1. Seleccione solamente el adaptador de red de **captura** o el adaptador de red conectado al puerto de conmutador configurado como destino de creación de reflejo de puerto.
2. Si no se ha instalado ATA todavía, compruebe que la opción Modo P esté habilitada. Si ya instaló el rol de portal de ATA, no haga clic en **Modo P**. Puesto que el servicio de la puerta de enlace de ATA coloca automáticamente la NIC en modo promiscuo, seleccionar esta opción podría ocasionar problemas.
3. Haga clic en **Nueva captura**.



1. En la ventana **Mostrar filtro** escriba el siguiente filtro: **KerberosV5 OR LDAP,** y luego haga clic en **Aplicar**.



1. Haga clic en **Iniciar** para iniciar la sesión de captura. Si el administrador no ve tráfico hacia y desde el controlador de dominio, revise la configuración de creación de reflejo del puerto.
2. Es importante asegurar que el administrador vea tráfico hacia y desde los controladores de dominio, como se muestra en la siguiente captura de pantalla.



1. Configuración de retroalimentación de ATA para Microsoft

Advanced Threat Analytics (ATA) puede recopilar datos de telemetría anónimos sobre ATA y, si se activa, se transferirán los datos a través de una conexión HTTPS a los servidores de Microsoft. Microsoft usa estos datos para que le ayuden a mejorar las versiones futuras de ATA. Esta opción está deshabilitada de manera predeterminada. Si decide habilitarla, ATA compartirá lo siguiente:

* Contadores de rendimiento tanto del Centro ATA como de la puerta de enlace de ATA
* Identificación (ID) de producto de las copias de ATA con licencia
* Fecha de implementación del Centro ATA
* Número de puertas de enlace de ATA implementadas
* La siguiente información anónima de Active Directory:
  + ID de dominio para el dominio que se lista primero en orden alfabético
  + Número de controladores de dominio
  + Número de controladores de dominio supervisados por ATA mediante la creación de reflejo de puerto
  + Número de sitios
  + Número de computadoras
  + Número de grupos
  + Número de usuarios
* Actividades sospechosas—Se recolectarán los siguientes datos anónimos para cada actividad sospechosa:
  + Tipo de actividad sospechosa
  + ID de actividad sospechosa
  + Estado
  + Hora de inicio y finalización
  + Entrada proporcionada

(No se recolectarán los nombres de computadoras, nombres de usuarios y direcciones IP.)

Lleve a cabo los siguientes pasos para comenzar a recolectar y enviar datos de telemetría a Microsoft:

1. Inicie sesión en la Consola de ATA.
2. En la barra de herramientas, haga clic en los tres puntos y luego en **Acerca de**.
3. Marque la casilla  **Envíenos información de uso para ayudarnos a mejorar su experiencia de cliente en el futuro**.

1. Al igual que las actividades sospechosas, las alertas del Centro de mantenimiento pueden descartarse o resolverse y se clasifican con un nivel de gravedad alto, medio o bajo. Si resuelve una alerta que el servicio ATA detecte como todavía activa, se moverá automáticamente a la lista de alertas Abiertas. Si el sistema detecta que ya no hay causa de alerta (la situación se corrigió), se moverá automáticamente a la lista de Resueltas. [↑](#footnote-ref-2)