ATAIS - Implementation Guide



Advanced Threat Analytics Implementation Services

Preparado para

Customer Name

10/19/2016

Versión 1 Draft

Preparado por

**[Update Author in Doc Properties]**

Contribuidores

**[Type Contributors Here]**

Revisión y Hoja de Firmas

Control de Cambio

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha | Autor | Versión | Referencia del Cambio |
|  |  | 1 | Borrador inicial para revision/discusión |
|  |  |  |  |
|  |  |  |  |

Revisores

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Versión Aprobada | Posición | Fecha |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Tabla de Contenidos

[1 Implementation Guide Summary 1](#_Toc454800137)

[1.1 Objectives 1](#_Toc454800138)

[2 Solution Requirements 2](#_Toc454800139)

[2.1 Sizing Requirements 2](#_Toc454800140)

[2.1.1 ATA Center 2](#_Toc454800141)

[2.1.2 ATA Lightweight Gateway 3](#_Toc454800142)

[2.1.3 ATA Gateway 4](#_Toc454800143)

[2.2 Hardware Requirements 4](#_Toc454800144)

[2.2.1 ATA Center 4](#_Toc454800145)

[2.2.2 ATA Lightweight Gateway 5](#_Toc454800146)

[2.2.3 ATA Gateway 5](#_Toc454800147)

[2.3 Software Requirements 7](#_Toc454800148)

[2.3.1 ATA Center 7](#_Toc454800149)

[2.3.2 ATA Lightweight Gateway 8](#_Toc454800150)

[2.3.3 ATA Gateway 9](#_Toc454800151)

[2.4 Pre-deployment Requirements 10](#_Toc454800152)

[3 Deployment 11](#_Toc454800153)

[3.1 Step 1: Installing the ATA Center 11](#_Toc454800154)

[3.1.1 Validating the Installation of the Center 13](#_Toc454800155)

[3.2 Step 2: Configure ATA Gateway Domain Connectivity Settings 14](#_Toc454800156)

[3.3 Step 3: Download the ATA Gateway Setup Package 15](#_Toc454800157)

[3.4 Step 4: Install the ATA Gateways 16](#_Toc454800158)

[3.4.1 Install the ATA Lightweight Gateway 16](#_Toc454800159)

[3.4.2 Install the ATA Gateway 17](#_Toc454800160)

[3.5 Step 5: Configure the ATA Gateways 19](#_Toc454800161)

[3.5.1 Configure the ATA Lightweight Gateway 19](#_Toc454800162)

[3.5.2 Configure the ATA Gateway 20](#_Toc454800163)

[3.5.3 Validating the ATA Gateway Installation 23](#_Toc454800164)

[3.6 Step 6: Configure Short-Term Lease Subnets 24](#_Toc454800165)

[3.7 Step 7: Configure the Honeytoken User 25](#_Toc454800166)

[3.8 Step 8: Post-Installation Information 25](#_Toc454800167)

[4 Appendix 26](#_Toc454800168)

[4.1 Configure Port Mirroring 26](#_Toc454800169)

[4.1.1 Supported Port Mirroring Options 27](#_Toc454800170)

[4.1.2 Hyper-V Virtual Switch – Windows Server 2012 27](#_Toc454800171)

[4.2 Configuring Security Information and Event Management (SIEM) Integration 28](#_Toc454800172)

[4.2.1 Configuring the ATA Gateway to Listen for and Accept SIEM Events 28](#_Toc454800173)

[4.2.2 Supported SIEM Solutions 29](#_Toc454800174)

[4.3 Configuring Windows Event Forwarding (WEF) 29](#_Toc454800175)

## Tabla de Tablas

[Table 1: Requirements - Center Sizing 2](#_Toc454800176)

[Table 2: Requirements – ATA Lightweight Gateway Sizing 3](#_Toc454800177)

[Table 2: Requirements – ATA Gateway Sizing 4](#_Toc454800178)

[Table 3: Requirements – ATA Center Hardware 4](#_Toc454800179)

[Table 4: Requirements – ATA Lightweight Gateway Hardware 5](#_Toc454800180)

[Table 4: Requirements – ATA Gateway Hardware 6](#_Toc454800181)

[Table 5: Requirements - Center Software 7](#_Toc454800182)

[Table 6: Requirements - Gateway Software 8](#_Toc454800183)

[Table 6: Requirements - Gateway Software 9](#_Toc454800184)

[Table 7: ATA Center - Installation Configuration 11](#_Toc454800185)

[Table 8: ATA Gateway - Domain Connectivity Settings 14](#_Toc454800186)

[Table 9: ATA Lightweight Gateway - Installation Configuration 16](#_Toc454800187)

[Table 9: ATA Gateway - Installation Configuration 18](#_Toc454800188)

[Table 10: ATA Gateway – Post-Installation Configuration 19](#_Toc454800189)

[Table 10: ATA Gateway – Post-Installation Configuration 21](#_Toc454800190)

[Table 11: Port Mirroring Options 27](#_Toc454800191)

## Tabla de Figuras

[Figure 1: ATA Center - Installation Configuration 13](#_Toc454800192)

[Figure 2: ATA Gateway - Domain Connectivity Settings 15](#_Toc454800193)

[Figure 3: ATA Lightweight Gateway - Installation Configuration 17](#_Toc454800194)

[Figure 3: ATA Gateway - Installation Configuration 19](#_Toc454800195)

[Figure 4: ATA Lightweight Gateway – Post-Installation Configuration 20](#_Toc454800196)

[Figure 4: ATA Gateway – Post-Installation Configuration 22](#_Toc454800197)

[Figure 5: Performance Monitor - Adding Counters 24](#_Toc454800198)

[Figure 6: ATA Detection Configuration 25](#_Toc454800199)

**Spell/grammar check is turned ON within all Services Delivery Method (SDM) Word templates -** Remember to turn off spell/grammar check before sending out the document if you want to avoid showing spelling and grammar red mark-ups. To turn this feature off, do the following:

1. Click on File
2. Click on the Options on the left
3. Click on Proofing
4. Scroll to bottom and check the two boxes shown below:



**To remove all the Visible Guidance (Hot Pink text with Grey Background) all at once:**

1. Click Ctrl H to open the Find and Replace box
2. Make sure your cursor is in the ‘Find what’ box.
3. Click on the More button at the bottom left
4. Click on the Format Button at the bottom left and select Style
5. Scroll down, locate select the “Visible Guidance”
6. Make sure the ‘Replace with’ box is empty:
7. Click ‘Replace All”
8. If not empty - click on the format button in the lower left hand corner. Scroll down and chose ‘(no style)’then replace all.

**IMPORTANT – Finalize This Document**

**REMOVE** all pink text, guidance, comments, changes, and hidden text in this document before submitting it to the customer. You can do this in two ways:

* **Save as PDF** and send the PDF version to the customer.   
  ~ OR ~
* **Inspect document and remove comments, revisions, any document properties you do not want included, personal information, and hidden text.** For guidance on how to do this, see [Remove hidden data and personal information from Office documents](http://office.microsoft.com/client/helppreview.aspx?AssetID=HA100375931033&QueryID=ALdFua2no0&respos=6&rt=2&ns=WINWORD&lcid=1033&pid=CH100487501033#3).

1. Resumen de Guía de Implementación

Este documento entrega información de la instalación para la implementación de Microsoft Advanced Threat Analytics (ATA). Este documento también complementa la Guía de Operaciones como parte de este proyecto.

* 1. Objectivos

Este documento cubre los siguientes tópicos para completar una implementación exitosa de ATA para Customer Name.

* Los requerimienos para el ATA Center y los ATA Gateway como se discutieron durante la fase de visión.
* La implementación de ATA basada en el acuerdo de configuración en el documento de diseño de la solución y los resultados de las fases de pruebas y estabilización.
* La configuración de la colección de eventos.
* La configuración de port mirroring dentro de Microsoft Hyper-V, si es requerido.

1. Requerimientos de la Solución

La siguiente sección describe los requerimientos discutidos durante la fase de visión de este proyecto y los acuerdos de configuración reflejados en el documento de diseño de la solución.

* 1. Requerimientos de Dimensionamiento
     1. ATA Center

La siguiente información entrega las pautas recomendadas para dimensionar el ATA Center. Esta información es dependiente del monto de tráfico de red que generen los controladores de dominio (tráfico desde y hacia) y el monto de datos relevantes (actividades sospechosas) que ATA detecta y almacena dentro de su base de datos. La siguiente tabla muestra las guía de dimensionamiento que ayudan a diseñar el tamaño necesario para el ATA Center.

EL ATA Center requiere un mínimo recomendado de 30 días de datos para aprender el comportamiento normal del usuario y la captura el análisis de comportamiento. El espacio requerido para la base de datos ATA por cada controlador de dominio está definido en la siguiente tabla, basado en las estadísticas de los controladores de dominios de Customer Name.

Esta metodología será utilizada para determinar las necesidades de cómputo del ATA Center. La información será documentada en la sección 2.4.1 de este documento.

Mayor detalle del dimensionamiento de ATA puede ser encontrado en el artículo TechNet “[ATA Capacity Planning](https://technet.microsoft.com/en-us/library/mt429323.aspx).”

Tabla 1: Requerimientos – Dimensionamiento ATA Center

| Paquetes Por Segundo\* | CPU (cores\*\*) | Memoria (GB) | Almacenamiento de Base de Datos por día (GB) | Almacenamiento de Base de Datos por mes (GB) | IOPS\*\*\* |
| --- | --- | --- | --- | --- | --- |
| 1.000 | 2 | 32 | 0,3 | 9 | 30 (100) |
| 10.000 | 4 | 48 | 3 | 90 | 200 (300) |
| 40.000 | 8 | 64 | 12 | 360 | 500 (1,000) |
| 100.000 | 12 | 96 | 30 | 900 | 1,000 (1,500) |
| 400.000 | 40 | 128 | 120 | 1,800 | 2,000 (2,500) |

\* Número diario total promedio de paquetes por Segundo desde todos los controladores de dominio que están siendo monitoreados por los ATA Gateways

\*\* Esto incluye cores Físicos, no cores hyperthreaded.

\*\*\* Numeros promedio (números peak)

**Notes:**

El ATA Center puede manejar un máximo agregado de 400.000 frames por Segundo (FPS) desde todos los controladores de dominio monitoreados.

El monto de almacenamiento indicado acá son valores netos. Siempre se debería contar el crecimiento y asegurar que el disco donde la base de datos resida tiene al menos 20% de espacio disponible.

Si el espacio disponible alcanza un mínimo de 20% o 100 GB, la colección de datos más antigua será borrada. Esto continuará ocurriendo hasta que solamente se tengan dos días de datos o que queden 5% o 50 GB de espacio disponible. En este punto, la colecta de datos dejará de funcionar.

La latencia del almacenamiento para actividades de lectura y escritura debería ser menor a 10 ms.

El ratio entre la actividades de lectura y escritura es aproximadamente 1:3 bajo los 100.000 paquetes por segundo y 1:6 sobre 100.000 paquetes por segundo.

* + 1. ATA Lightweight Gateway

Un ATA Lightweight Gateway se instala directamente sobre el controlador de dominio y monitora el tráfico directamente. Es recomendado que se utilice ATA Lightweight Gateway en vez de ATA Gateway cuando sea posible, esto es, cuando los controladores de dominio cumplan con el dimensionamiento indicado en la tabla de más abajo. Un ATA Lightweight Gateway puede soportar el monitoreo de un controlador de dominio.

La siguiente tabla entrega algunas sugerencias a alto nivel relacionadas a como dimensionar los controladores de dominio basado en el monto de tráfico enviado y recibido. Más información sobre dimensionamiento de ATA puede ser encontrado en el siguiente artículo de TechNet “[ATA Capacity Planning](https://technet.microsoft.com/en-us/library/mt429323.aspx).”

Tabla 2: Requerimientos – Dimensionamiento de ATA Lightweight Gateway

| Paquetes Por Segundo\* | CPU (cores\*\*) | Memoria (GB) |
| --- | --- | --- |
| 1.000 | 2 | 6 |
| 5.000 | 6 | 16 |
| 10.000 | 10 | 24 |

**\*** Número total promedio en horario laboral de paquetes por segundo desde los controladores de dominio que está siendo monitoreado por un ATA Lightweight Gateway específico.

**\*\*** Hyperthreading debe ser deshabilitado.

* + 1. ATA Gateway

Un ATA Gateway puede soportar el monitoreo de múltiples controladores de dominio, dependiendo del monto de tráfico de red de los DC que están siendo monitoreados. La siguiente tabla entrega algunas sugerencias a alto nivel sobre como dimensionar los ATA Gateway basado en el monto de tráfico de red enviado y recibido. Más información sobre dimensionamiento de ATA puede ser encontrado en el siguiente artículo de TechNet “[ATA Capacity Planning](https://docs.microsoft.com/en-us/advanced-threat-analytics/plan-design/ata-capacity-planning).”

Tabla 3: Requerimientos – Dimensionamiento de ATA Gateway

| Paquetes Per Segundo\* | CPU (cores\*\*) | Memoria (GB)\*\*\* |
| --- | --- | --- |
| 1.000 | 1 | 6 |
| 5.000 | 2 | 10 |
| 10.000 | 3 | 12 |
| 20.000 | 6 | 24 |
| 50.000 | 16 | 48 |

**\*** Número diario total promedio de paquetes por Segundo desde todos los controladores de dominio que están siendo monitoreados por los ATA Gateways. Además, el monto total del tráfico del controlador de dominio con port mirroring no puede exceder la capacidad de la NIC de captura del ATA Gateway.

**\*\*** Número total de núcleos no hyper-threading que tiene instalado el controlador de dominio. Hyper-threading está aceptado para los ATA Lightweight Gateway, cuando se planee la capacidad, deberían contabilizar los núcleos reales y no los núcleos hypert-threading.

**\*\*\*** Monto total dememoria que tiene instalada el controlador de dominio.

* 1. Requerimientos de Hardware
     1. ATA Center

El número de controladores de domino de Customer Name que son monitoreados y la carga de cada uno de ellos que indicarán los requerimientos de hardware.

La siguiente tabla muestra los requerimientos bases para el ATA Center.

Tabla 3: Requerimientos – Hardware de ATA Center

| Componente | Requerimientos de Hardware para ATA Center |
| --- | --- |
| Procesador | Referirse a los requerimientos de dimensionamiento |
| Memoria | Referirse a los requerimientos de dimensionamiento |
| Espacio disponible en disco  Almacenamiento de Base de datos | Referirse a los requerimientos de dimensionamiento |
| Red | La comunicación entre el ATA Center y el ATA Gateway es encriptada utilizando Secure Sockets Layer (SSL) sobre el puerto 443. Adicionalmente, la consola de Administración de ATA se ejecuta sobre Microsoft Internet Information Services (IIS) y la seguridad es mejorada utilizando SSL sobre el puerto 443. Se requieren **dos direcciones IP**. El servicio de ATA Center está asociado al puerto 443 sobre la primera dirección IP y el IIS estará asociado al puerto 443 en la segunda dirección IP. Se deben considerar los requerimientos de puertos de red en la siguiente tabla.  **Nota:** Se debe asegurar una conexión de red Segura y estable entre el ATA Center y el ATA Gateway. Ver los requerimientos de memoria para ATA Gateway.  **Nota:** Subredes con arriendo a corto plazo   * Identificar las subredes que son reasignadas entre dispositivos en un periodo muy corto de tiempo (segundos o minutos). ATA reducirá el caché del tiempo de vida para las direcciones IP de esas subredes para acomodar la reasignación rápida entre dispositivos. Virtual private network (VPN) o redes inalámbricas son ejemplos comunes de subredes con arriendo a corto plazo. |
| Virtualización | La instalación del ATA Center sobre una máquina virtual (VM) está soportada. |
| BIOS | La bases de datos de ATA require que Customer Name DESHABILITE non-uniform memory access (NUMA) en el BIOS. Los sistemas podrían referirse a NUMA como Node Interleaving, en ese caso se deberá HABILITAR Node Interleaving. |

* + 1. ATA Lightweight Gateway

Un ATA Lightweight Gateway soportará y monitoreará solo el controlador de dominio donde esta instalado.

Tabla 4: Requerimientos – Hardware de ATA Lightweight Gateway

| Nombre Controlador de Dominio | Paquetes por Segundo | CPU (Núcleos) | Memoria (GB) |
| --- | --- | --- | --- |
| NombreDC | X,xxx | # Núcleos CPU | Memoria instalada |

* + 1. ATA Gateway

Un ATA gateway puede soportar el monitoreo de multiples controladores de dominio, dependiendo del monto de tráfico de red sobre los controladores de dominio que están siendo monitoreados.

Tabla 4: Requerimientos – Hardware de ATA Gateway

| Componente | Requerimientos de Hardware de ATA Gateway |
| --- | --- |
| Procesador | Referirse a los requerimientos de dimensionamiento |
| Memory | Referirse a los requerimientos de dimensionamiento  **Nota:** El ATA Gateway utiliza su memoria para almacenar los datos capturados y enviarlos al ATA Center. Existe una configuración por defecto de 1.000.000 de entidades y es configurable. Dependiendo de la carga del controlador de dominio conectado al ATA Gateway se puede generar una gran cantidad de datos.  **Precaución:** Si las comunicaciones entre el ATA Center y el ATA Gateway son interrumpidas, el ATA Gateway almacenará los datos en memoria. 1.000.000 de entidades pueden ocupar hasta 5 GB de memoria. Una vez que el límite es alcanzado, se detendrá la captura de tráfico de red hasta que la comunicación sea restaurada con el ATA Center. Esto puede ser horas o minutos dependiendo de la carga del controlador de dominio. |
| Espacio en disco disponible | Referirse a los requerimientos de dimensionamiento |
| Red | El ATA Gateway requiere dos o más adaptadores de red.  **Adaptador de Administración**: Será usado para comunicaciones sobre la red de la compañía. Este adaptador debería ser configurado con lo siguiente:   * Dirección IP estática incluyendo el default gateway. * Servidor Domain Name System (DNS) preferido y alternativo. * “DNS suffix for this connection” debería ser el nombre de DNS del dominio monitoreado.   **Adaptador de Captura**: Será usado para capturar tráfico de red desde y hacia los controladores de dominio.   * Se debe configurar port mirroring para el adaptador de captura el destino del tráfico de red del controlador de dominio. * Configurar una dirección IP estática, no ruteable, para el ambiente sin default gateway y sin servidores DNS. Por ejemplo, 1.1.1.1/8. * Esto asegurará que la tarjeta de red de captura, colectará el monto máximo de tráfico y la tarjeta de red de administración sea usada para enviar y recibir el tráfico de red requerido.   **Nota:** Subredes de arriendo de corto plazo  Se deben identificar las subredes en las cuales las direcciones IP son reasignadas entre dispositivos dentro de un periodo corto de tiempo (segundos o minutos). ATA reduce el tiempo de vida de la caché para las direcciones IP en esas subredes para acomodar la reasignación rápida entre dispositivos. Las redes inalámbricas o VPN son ejemplos comunes de subredes de arriendo de corto plazo. |
| Virtualización | La instalación del ATA Gateway sobre una VM es soportado cuando el controlador de dominio monitoreado también está ejecutándose como VM en el mismo host de virtualización.  **Nota Importante:** No instale el KB 3047154 sobre el host de virtualizaicón. Esto podría causar que el port mirroring deje de funcionar apropiadamente. |

* 1. Requerimientos de Software
     1. ATA Center

Esta sección entrega requerimientos de software para el ATA Center.

Tabla 5: Requerimientos – Software ATA Center

| Componente | Requerimientos de Software de ATA Center |
| --- | --- |
| Certificados | ATA Center requiere certificados para los siguientes servicios:   * IIS – certificado de servidor web * Servicio de ATA Center – certificado de autenticación de servidor |
| Sistema Operativo | Windows Server 2012 R2 Standard o Datacenter  El ATA Center **NO PUEDE** ser instalado sobre un controlador de dominio. |
| Membresía de dominio o grupo de trabajo | El ATA Center puede ser instalado sobre un servidor que sea miembro de un dominio o de un grupo de trabajo.  Es altamente recomendable que sea distribuido en una configuración de grupo de trabajo. |
| Cuenta de usuario | **Administrador local (grupo de trabajo)**  **Cuenta de usuario estándar (unido al dominio):** Agregada al grupo local administrator, y al grupo ATA Administrators |
| Componentes | Los siguientes componentes son instalados y configurados durante la instalación del ATA Center:   * IIS * MongoDB * Servicio de ATA Center service y sitio IIS de administración de ATA * Grupo de colección de datos personalizados de Performance Monitor * Certificado X.509 es recomendado y será emitido por la infraestructura interna de llaves públicas. Los certificados auto firmados son sólo recomendados para propósitos de prueba. |
| Soporte de navegadores | El acceso a la consola de administración de ATA se hace por medio de navegadores. Los siguientes son los soportados:   * Internet Explorer versión 10 o superior. * Google Chrome 40 * Resolución minima de pantalla de 1700 pixeles |
| Actualizaciones Microsoft | Se debe asegurar que las actualizaciones de Microsoft hayan sido instaladas sobre el servidor.  Instalar el [KB 2934520](https://support.microsoft.com/en-us/kb/2934520) es un pre requisito. |

* + 1. ATA Lightweight Gateway

Esta sección entrega los requerimientos de software para el ATA Lightweight Gateway.

Tabla 6: Requerimientos – Software de ATA Gateway

| Componente | Requerimientos de software de ATA Lightweight Gateway |
| --- | --- |
| Certificados | ATA Lightweight Gateway requiere certificados para el siguiente servicio:   * Un certificado que soporte **Server Authentication** es requerido para que sea instalado en el almacenamiento de computador del ATA Gateway en el almacenamiento de computador local. Este certificado debe ser confiable para el ATA Center. |
| Sistema operativo | El ATA Lightweight Gateway soporta la instalación en un controlador de dominio corriendo Windows Server 2008 R2, Windows Server 2012 o Windows Server 2012 R2.  El controlador de dominio puede ser un read-only domain controller (RODC).  El controlador de dominio no puede estar ejecutando Server Core. |
| Cuentas de usuarios | **Cuenta de Servicio estándar**: Usada para consultar al Active Directory para indexar y catalogar objetos o entidades. (Conectividad de dominio)  **Cuenta Honeytoken**: Usa un security identifier (SID) (opcional): Una cuenta honeytoken es un usuario que no tiene actividades de red. Esta cuenta será configurada como el usuario honeytoken de ATA. Para configurar el usuario honeytoken se necesitará el DIS de la cuenta de usuario, no el nombre de usuario.  **Opcional:** La cuenta de servicio estándar debería tener permisos de sólo lectura para el contenedor de Objetos Eliminados. Esto permitirá a ATA detector el borrado masivo de objetos en el dominio. Para información sobre configurar permisos de solo lectura sobre el contenedor Objetos Eliminados, ver la sección **Changing permissions on a deleted object container** en el tópico [View or Set Permissions on a Directory Object](https://technet.microsoft.com/library/cc816824(v=ws.10).aspx). |
| Componentes | Los siguientes conponentes se instalan y configuran durante la instalación de ATA Gateway:   * Servicio ATA Lightweight Gateway * Microsoft Visual C++ 2013 Redistributable * Grupo de colección de datos personalizados de Performance Monitor |
| Actualizaciones Microsoft | Ejecutar las actualizaciones de Windows y asegurarse que las actualizaciones **Important** hayan sido instaladas. |
| Sniffers de red | No se debe instalar Message Analyzer, Wireshark u otro software de captura de red sobre el ATA Lightweight Gateway. Si se necesita capturar el tráfico de red, se debe instalar y usar Microsoft Network Monitor 3.4. |

* + 1. ATA Gateway

This section provides the software requirements for the ATA Gateway.

Table 6: Requirements - Gateway Software

| Componente | Requerimientos de Software de ATA Gateway |
| --- | --- |
| Certificados | ATA Gateway requiere certificados para los siguientes servicios:   * Un certificado que soporte **Server Authentication** es requerido para que sea instalado en el almacenamiento de computador del ATA Gateway en el almacenamiento de computador local. Este certificado debe ser confiable para el ATA Center. |
| Sistema operativo | Windows Server 2012 R2 Standard o Datacenter |
| Membresía de dominio o grupo de trabajo | El ATA Center puede ser instalado sobre un servidor que sea miembro de un dominio o de un grupo de trabajo.  Es altamente recomendable que sea distribuido en una configuración de grupo de trabajo. |
| Cuentas de usuarios | **Administrador local (grupo de trabajo)**  **Cuenta de usuario estándar (unido al dominio):** Agregada al grupo local administrator, y al grupo ATA Administrators  **Cuenta de Servicio estándar**: Usada para consultar al Active Directory para indexar y catalogar objetos o entidades. (Conectividad de dominio)  **Cuenta Honeytoken**: Usa un security identifier (SID) (opcional): Una cuenta honeytoken es un usuario que no tiene actividades de red. Esta cuenta será configurada como el usuario honeytoken de ATA. Para configurar el usuario honeytoken se necesitará el DIS de la cuenta de usuario, no el nombre de usuario.  **Opcional:** La cuenta de servicio estándar debería tener permisos de sólo lectura para el contenedor de Objetos Eliminados. Esto permitirá a ATA detector el borrado masivo de objetos en el dominio. Para información sobre configurar permisos de solo lectura sobre el contenedor Objetos Eliminados, ver la sección **Changing permissions on a deleted object container** en el tópico [View or Set Permissions on a Directory Object](https://technet.microsoft.com/library/cc816824(v=ws.10).aspx). |
| Components | Los siguientes componentes son instalados y configurados durante la instalación del ATA Center:   * KB 3047154 (No instale KB 3047154 sobre un host de virtualización. Esto podría causar que el port mirroring no funcione correctamente.) * Servicio ATA Gateway * Microsoft Visual C++ 2013 Redistributable * Grupo de colección de datos personalizados de Performance Monitor |
| Actualizaciones Microsoft | Ejecutar las actualizaciones de Windows y asegurarse que las actualizaciones **Important** hayan sido instaladas. Antes de instalar el ATA Gateway confirme que la siguiente actualización haya sido instalada, [KB 2919355](https://support.microsoft.com/en-us/kb/2919355/). Si la actualización no está instalada, se debe instalar antes de instalar el servicio de ATA Gateway.  Instalar [KB 2934520](https://support.microsoft.com/en-us/kb/2934520) como un pre requisito. |
| Sniffers de red | No se debe instalar Message Analyzer, Wireshark u otro software de captura de red sobre el ATA Lightweight Gateway. Si se necesita capturar el tráfico de red, se debe instalar y usar Microsoft Network Monitor 3.4. |

* 1. Requerimientos de Pre Instalación

1. De acuerdo a los requerimientos de software de la sección previa, se debe validar que el [KB 2934520](https://support.microsoft.com/en-us/kb/2934520) esté instalado sobre los servidores ATA Center server y ATA Gateway antes de comenzar con la instalación. De otra manera, la instalación de ATA instalará esta actualización y se requerirá reiniciar en medio de la instalación de ATA.
2. Sobre el ATA Gateway, se debe asegurar que el [KB 2919355](http://support.microsoft.com/kb/2919355/) haya sido instalado. Se debe ejecutar el siguiente comando PowerShell para chequear si el hotfix está instalado: Get-HotFix -Id kb2919355.
3. Revisar el apendice de este documento para información adicional sobre la configuración de port mirroring. La sección de implementación de este document asume que el port mirroring ha sido configurado y se encuentra operativo.
4. Para validar el port mirroring, se debe revisar la Guía de Operación de ATAIS que se entrega como parte de este proyecto.
5. Despliegue

La siguiente sección cubre los pasos de instalación que se deben seguir para distribuir ATA dentro de Customer Name.

* 1. Paso 1: Instalación de ATA Center

Después que se ha verificado que el servidor reúne los requerimientos, el administrador puede proceder con la instalación del ATA Center.

1. Iniciar sesión sobre el ATA Center con un usuario que sea miembro del grupo local administrators.
2. Desde una consola de comandos con privilegios de administrador, se debe ejecutar Microsoft ATA Center Setup.EXE y seguir el asistente de instalación.
3. Sobre la página **Welcome**, se debe seleccionar el lenguaje y hacer clic en **Next**.
4. Leer el Acuerdo de Licencia para el Usuario Final y si acepta los téminos, hacer clic en **Next**.
5. En la página **Center Configuration**, ingresar la información basada en el documento de Diseño de la Solución.

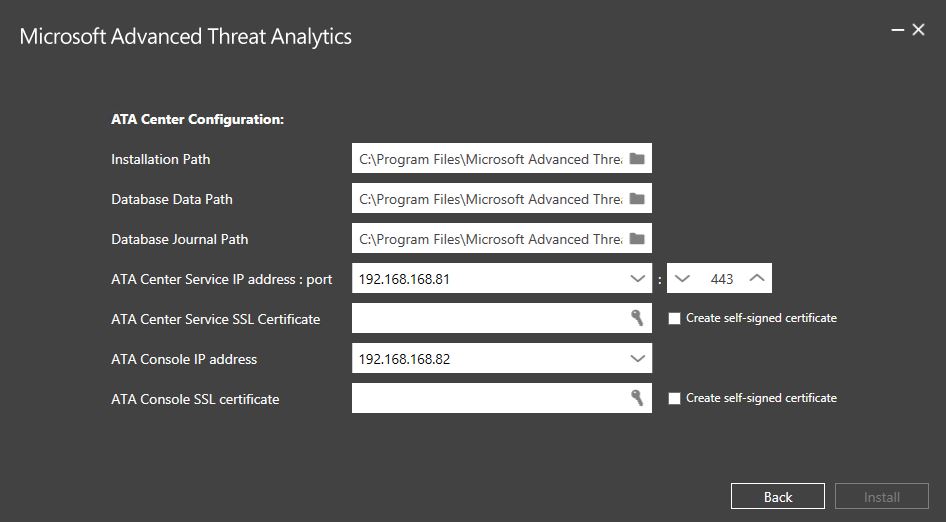
**Instructions:** Update the following table to record the customer specific installation configuration. This will include certificate information, network ports, or default install locations if they are modified discussed during the design phase. Remove the highlights if default is not changed.

Table 7: ATA Center - Installation Configuration

| Campo | Descripción | Comentarios |
| --- | --- | --- |
| Ruta de Instalación | Esta es la ubicación donde el ATA Center será instalado. Por defecto, la ruta es %programfiles%\Microsoft Advanced Threat Analytics\Center | Se debe mantener el valor por detecto |
| Ruta de la Base de datos | Esta es la ubicación donde los archivos de la base de datos MongoDB serán ubicados. Por defecto, la ruta es %programfiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\data | Cambiar la ubicación a una donde se tenga espacio para crecer basado en el dimensionamiento.   |  | | --- | | System_CAPS_noteNota | | En los ambientes de producción el administrador debería utilizar la unidad que tenga espacio suficiente basado en la planificación de las capacidades.  Para implementaciones grandes, la base de datos debería estar en un disco físico, esto mejorará el rendimiento. | |
| Ruta de díario de Base de datos | Esta es la ubicación donde los archivos de la base de datos MongoDB serán ubicados. Por defecto, la ruta es %programfiles%\Microsoft Advanced Threat Analytics\Center\MongoDB\bin\data\journal | Para ambientes grandes, el registro diario de la base de datos debería estar en un disco distinto de la base de datos o del sistema. Cambie la ubicación del lugar donde estará el registro diario de la base de datos. |
| Dirección IP : Puerto del Servicio de ATA Center | Esta es la direción IP por la que el servicio de ATA Center se comunicará con el/los ATA Gateway.  Puerto por defecto: 443 | Seleccione la dirección IP que será utilizada por el servicio de ATA Center.  La dirección IP y el puerto del servicio de ATA Center no pueden ser los mismos que para la consola de ATA. Se debe cambiar el puerto de la consola ATA. |
| Certificado SSL del servicio de ATA Center Service | Este es el certificado que será usado por el servicio de ATA Center. | Haga clic sobre el icono de llave para seleccionar un certificado instalado o haga clic en el check para generar un certificado auto firmado si se están instalando un ambiente de laboratorio. |
| Dirección IP de la consola ATA | Esta es la dirección IP que será usada por el IIS para la conola ATA. | |  | | --- | | Seleccione la dirección IP que será utilizada por la consola de ATA.  System_CAPS_noteNota | | Anotar esta direccion IP para hacer fácil el acceso a la consola ATA desde el ATA Gateway. | |
| Certificado SSL para la consola ATA | Este es el certificado usado por el IIS. | Haga clic sobre el icono de llave para seleccionar un certificado instalado o haga clic en el check para generar un certificado auto firmado si se están instalando un ambiente de laboratorio. |

Ver el siguiente ejemplo:

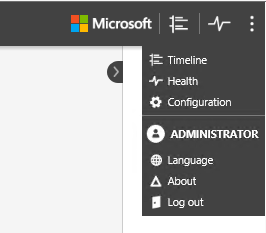
Figura 1: ATA Center – Configuración de Instalación



1. Haga clic en **Install** para instalar ATA y sus componentes y crear la conexión entre el ATA Center ya consola de ATA.
2. Cuando la instalación se complete, haga clic en **Launch para conectarse a la consola** ATA.
   * 1. Validación de la instalación del ATA Center
3. Verificar que el servicio Microsoft ATA Center esté ejecutándose por revisando la consola de servicios. Esto se hace escribiente Services.msc desde el **ícono de Inicio de Windows** y seleccionando **Run**.
4. Sobre el escritorio, haga clic en el acceso directo de Microsoft ATA para conectarse a la consola. Se debe iniciar sesión con el mismo usuario y las mismas credenciales usadas para instalar el ATA Center. La primera vez que se inicie sesión en la consola ATA, automáticamente se redireccionará a la página **Domain connectivity settings** para continuar con la configuración y la implementación de ATA Gateway.
5. Se debe revisar el archivo **Microsoft.Tri.Center-Errors.log** el que se encuentra en la siguiente ubicación por defecto: %programfiles%\Microsoft Advanced Threat Analytics\Center\Logs.
   1. Paso 2: Configurar ajustes de conctividad de dominio del ATA Gateway

El ajuste en la sección de configuraciones de conectividad de dominio aplica a los ATA Gateway administrados por el ATA Center.

1. Abrir la consola ATA e iniciar sesión.
2. La primera vez que se inicie sesión en la consola ATA después de la instalación del ATA Center, automáticamente se redirigirá a la página de configuración de ATA Gateways. Si, posterior a eso, se necesita modificar la configuración, haga clic en el ícono de Ajustes y seleccione **Configuration**.



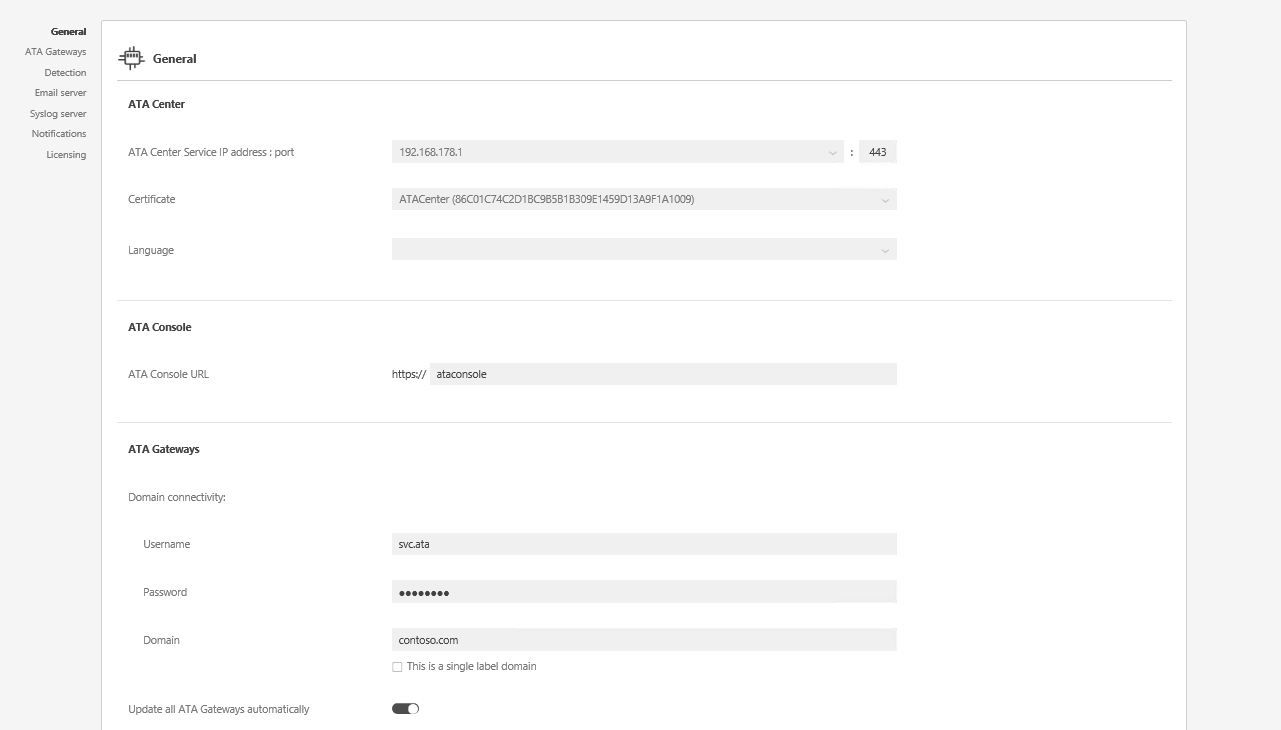
En la página **Gateways**, haga clic sobre **Domain connectivity settings**, ingrese la siguiente información y haga clic en **Save**.

Tabla 8: ATA Gateway – Ajustes de conectividad de dominio

| Campo | Comentarios |
| --- | --- |
| Nombre de Usuario (requerido) | Ingresar el nombre del usuario con acceso de solo lectura escogido durante el diseño de la solución. |
| Contraseña (requerido) | Ingrese la contraseña del usuario de solo lectura.   |  | | --- | | System_CAPS_note**Nota** | | Asegurarse que la contraseña sea correcta. Si se ingresa una contraseña incorrecta, el servicio ATA se detendrá sobre los servidores ATA Gateway. | |
| Dominio (requerido) | Ingrese el dominio del usuario de solo lectura, por ejemplo, **contoso.com**.   |  | | --- | | System_CAPS_note**Nota** | | Es importante que se ingrese el fully qualified domain name (FQDN) del dominio donde se ubica el usuario. Por ejemplo, si la cuenta de usuario está en el dominio corp.contoso.com, se necesita escribir corp.contoso.com no contoso.com | |

Ver el siguiente ejemplo:

Figura 2: ATA Gateway – Ajustes de Conectividad de Dominio



* 1. Paso 3: Descarga del paquete de instalación de ATA Gateway

Después de configurar los ajustes de conectividad de dominio, el administrador puede descargar el paquete de instalación del ATA Gateway.

1. Iniciar sesión sobre el servidor ATA Gateway.
2. Sobre la máquina de ATA Gateway, abre un navegador e ingrese la dirección IP e ingrese la dirección IP que se configuró en el ATA Center para la consola ATA. Cuando se abra la consola ATA, haga clic en el ícono de ajustes y seleccione **Configuration**.
3. En la pestaña **ATA Gateways**, haga clic en **Download ATA Gateway Setup**.
4. Guardar el paquete localmente.

El archivo .zip incluye lo siguiente:

* Instalador de ATA Gateway
* Archivo de ajustes de configuración con la información requerida para conectarse al ATA Center
  1. Paso 4: Instalar el ATA Gateway
     1. Instalar el ATA Lightweight Gateway

El ATA Lightweight Gateway se instala directamente sobre el controlador de dominio que será monitoreado. Se deben realizar los siguientes pasos en el controlador de dominio.

1. Extraer los archivos desde el archivo .zip.
2. Desde una consola de comando con privilegios de administrador, ejecutar Microsoft ATA Gateway Setup.exe y seguir el asistente de instalación.
3. Sobre la página **Welcome**, Selecionar el idioma y hace clic en **Next**.
4. En el asistente de tipo de instalación, sólo la opción ATA Lightweight Gateway estará desplegada, hacer clic en **Next**.
5. Bajo **ATA Gateway Configuration**, ingresar la siguiente información basada en el ambiente:

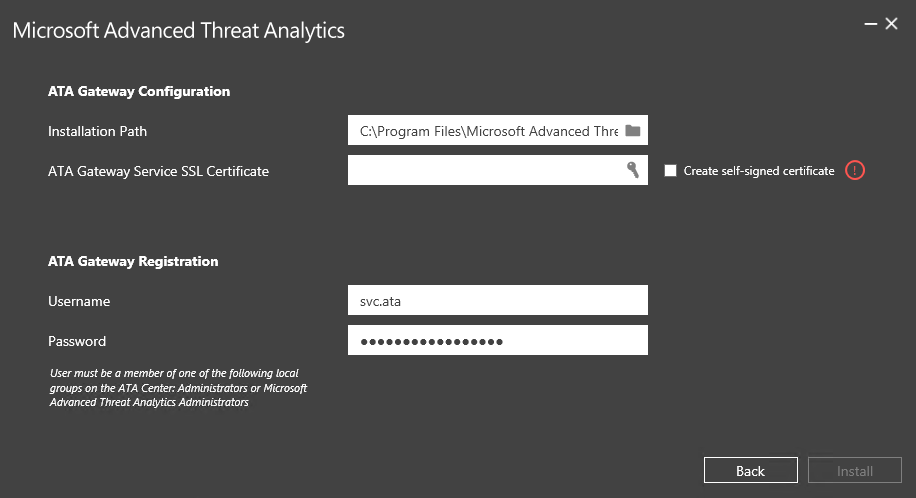
**Instructions:** Update the following table to record the customer specific installation configuration. This will include certificate information and default install locations if they are modified discussed during the design phase. Remove the highlights if default is not changed.

Tabla 9: ATA Lightweight Gateway – Configuración de Instalación

| Campo | Descripción | Comentarios |
| --- | --- | --- |
| Ruta de instalación | Esta es la ubicación donde el ATA Gateway será instalado. Por defecto la ruta es %programfiles%\Microsoft Advanced Threat Analytics\Gateway | Mantener el valor por defecto. |
| Certificado para el servicio SSL de ATA Gateway | Este es el certificado que será utilizado por el ATA Gateway. | Usar un certificado auto firmado sólo para propósitos de laboratorio. |
| Registro de ATA Gateway | Ingrese el nombre de usuario y contraseña del administrador de ATA. | Para que el ATA Gateway se registre con el ATA Center, ingrese el nombre de usuario y la contraseña del usuario que instaló el ATA Center. Este usuario debe ser miembro de uno de los siguientes grupos sobre el ATA Center.   * Administrators * ATA administrators  |  | | --- | | System_CAPS_note**Nota** | | Esas credenciales son solo usadas para el registro y no son almacenadas por el ATA. | |

Ver el siguiente ejemplo:

Figura 3: ATA Lightweight Gateway – Ajustes de Configuración



1. Después que la instalación se complete, haga clic en **Finish.**
2. Desde otra máquina, abrir un navegador e iniciar sesión en la consola ATA.
   * 1. Instalar el ATA Gateway

Antes de instalar el ATA Gateway, se debe validar que el port mirroring está configurado y que el ATA Gateway puede ver el tráfico desde y hacia los controladores de dominio que serán monitoreados por cada ATA Gateway. Ver el documento de Guía de Operaciones de este Proyecto para verificar el port mirroring.

1. Extraer los archivos desde el archivo .zip.
2. Desde una consola de comando con privilegios de administrador, ejecutar Microsoft ATA Gateway Setup.exe y seguir el asistente de instalación.
3. Sobre la página **Welcome**, Selecionar el idioma y hace clic en **Next**.
4. Bajo **ATA Gateway Configuration**, ingresar la siguiente información basada en el ambiente:

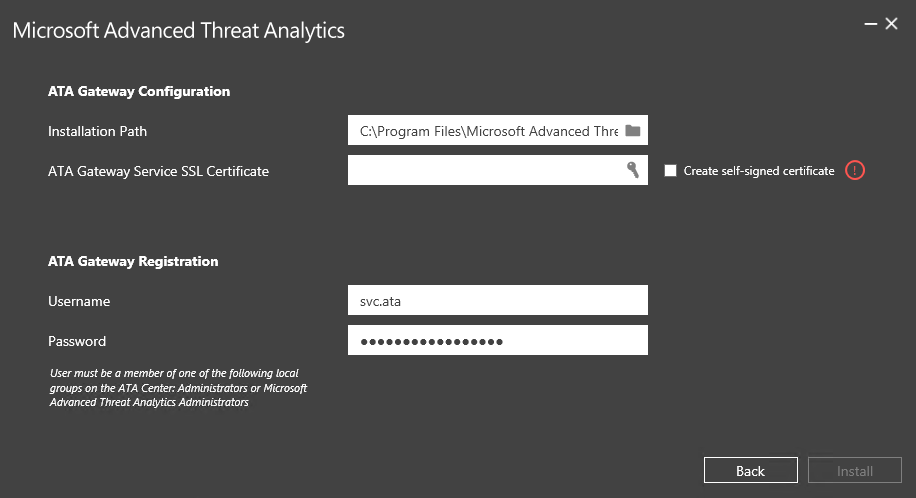
**Instructions:** Update the following table to record the customer specific installation configuration. This will include certificate information and default install locations if they are modified discussed during the design phase. Remove the highlights if default is not changed.

Tabla 13: ATA Gateway – Configuración de Instalación

| Campo | Descripción | Comentarios |
| --- | --- | --- |
| Ruta de instalación | Esta es la ubicación donde el ATA Gateway será instalado. Por defecto la ruta es %programfiles%\Microsoft Advanced Threat Analytics\Gateway | Mantener el valor por defecto. |
| Certificado para el servicio SSL de ATA Gateway | Este es el certificado que será utilizado por el ATA Gateway. | Usar un certificado auto firmado sólo para propósitos de laboratorio. |
| Registro de ATA Gateway | Ingrese el nombre de usuario y contraseña del administrador de ATA. | Para que el ATA Gateway se registre con el ATA Center, ingrese el nombre de usuario y la contraseña del usuario que instaló el ATA Center. Este usuario debe ser miembro de uno de los siguientes grupos sobre el ATA Center.   * Administrators * ATA administrators  |  | | --- | | System_CAPS_note**Nota** | | Esas credenciales son solo usadas para el registro y no son almacenadas por el ATA. | |

Ver el siguiente ejemplo:

Figura 4: ATA Gateway – Configuración de Instalación



1. Después de que se complete la instalación, haga clic en **Launch para abrir un navegador e iniciar sesión sobre la consola** ATA.
   1. Paso 5: Configuración de ATA Gateway
      1. Configuración del ATA Lightweight Gateway

Después que el ATA Lightweight Gateway se instale, se deben realizar los siguientes pasos para configurar los ajustes para el ATA Lightweight Gateway.

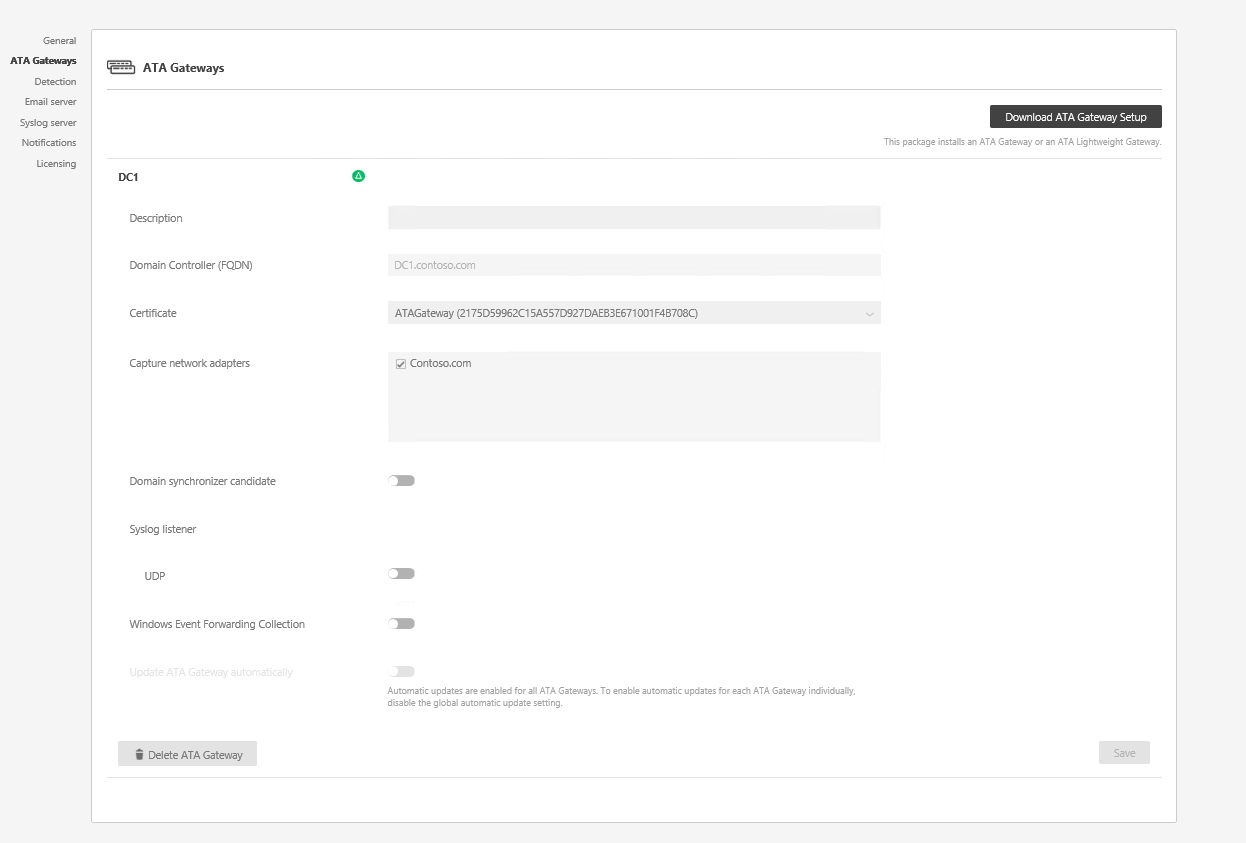
1. Sobre la máquina de ATA Gateway, en la consola ATA, haga clic en **Configuration** y seleccione la página **ATA Gateways**
2. Ingresar la siguiente configuración:

Tabla 14: ATA Gateway – Configuración Post-Instalación

| Campo | Descripción | Comentarios |
| --- | --- | --- |
| Descripción | Ingresar una descripción del ATA Gateway (opcional). |  |
| Controladores de dominio (requerido)  Para información adicional sobre la lista de controladores, ver lo siguiente. | El FQDN del controlador de dominio ya está ingresado |  |
| Adapatador de captura de red (requerido) | Por defecto, todos los adapatadores de red son seleccionados |  |

Ver el siguiente ejemplo:

Figura 5: ATA Lightweight Gateway – Configuración Post-Installación



1. Por defecto, los ATA Lightweight Gateway no son candidatos a Domain Synchronizer porque ellos son instalados tipicamente en sucursales y sobre controladores de dominio pequeños. Si este ATA Lightweight Gateway será domain synchronizer, seleccionar la opción, y hace clic en **Save**.
2. Los cambios en la configuración serán aplicaddos al ATA Gateway en la siguiente sincronización entre el ATA Gateway y el ATA Center.
   * 1. Configurar el ATA Gateway

Después que el ATA Gateway se instale, se deben realizar los siguientes pasos para configurar los ajustes para el ATA Gateway.

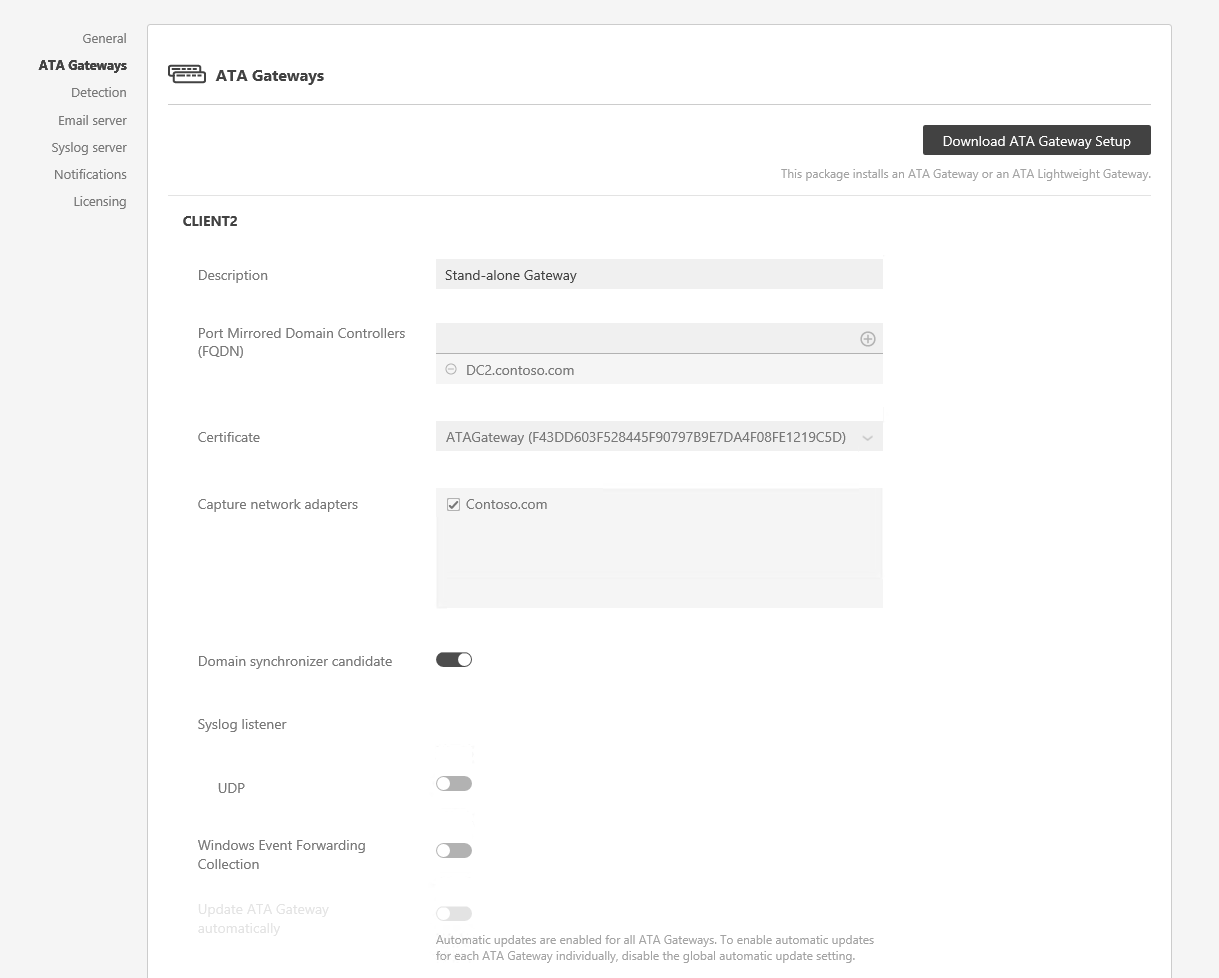
1. Sobre la máquina de ATA Gateway, en la consola ATA, haga clic en **Configuration** y seleccione la página **ATA Gateways**
2. Ingresar la siguiente configuración:

Tabla 15: ATA Gateway – Configuración Post-Instalación

| Campo | Descripción | Comentarios |
| --- | --- | --- |
| Descripción | Ingresar una descripción del ATA Gateway (opcional). |  |
| Controladores de dominio (requerido)  Para información adicional sobre la lista de controladores, ver lo siguiente. | Ingresar el FQDN del controlador de dominio y haga clic en el signo más para agregarlo a la lista. Por ejemplo, **dc01.contoso.com** | Los objetos en el primer controlador de dominio en la lista se sincronizarán con el protocolo de consulta Lightweight Directory Access Protocol (LDAP). Dependiendo del tamaño del dominio, esto podría tomar algún tiempo.   |  | | --- | | System_CAPS_note**Nota** | | Se debe asegurar que el primer controlador de dominio **no es** un RODC.  RODC deberían ser agregados sólo después que se complete la sincronización inicial. | |
| Adapatador de captura de red (requerido) | Seleccionar el adaptador de red que está conectado al switch que se configuró como el destino del port mirroring para recibir el tráfico del controlador de dominio. | Seleccionar el adaptador de red de captura. |

Ver el siguiente ejemplo:

Figura 6: ATA Gateway – Configuración Post-Instalación



1. Hacer clic en **Save**.
2. Tomará unos minutos para que el servicio de ATA Gateway se inicie la primera vez debido a que construye la cache de los analizadores de captura de red usados por el ATA Gateway.
3. Los cambios en la configuración serán aplicados al ATA Gateway en la siguiente sincronización entre el ATA Gateway y el ATA Center.

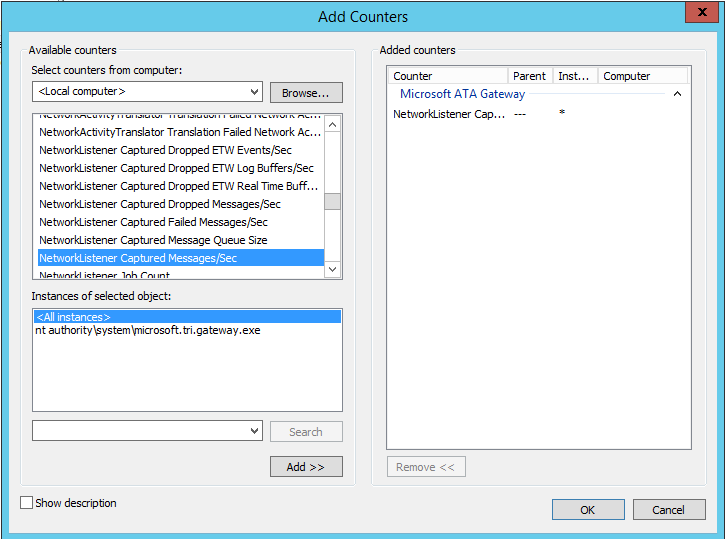
La siguiente información se aplica a los servidores que se ingresen en la lista de controladores de dominio:

* El primer controlador de dominio en la lista será usado por el ATA Gateway para sincronizar los objetos en el dominio a través de una consulta LDAP. Despendiendo del tamaño del dominio, esto podría tomar algún tiempo.
* El controlador del dominio, cuyo tráfico está siendo monitoreado por medio de port mirroring por el ATA Gateway, debe estar listado en la lista de controladores de dominio. Si no está listado en la lista de controladores de dominio, la detección de actividades sospechosas podría no funcionar como se espera.
* Se debe asegurar que el primer controlador de dominio **no es** un RODC.
* Los RODC podrían ser agregados sólo después que se complete la sincronización inicial.
* Al menos un controlador de dominio en la lista debe ser servidor de catálogo global. Esto le facilitará a ATA resolver objetos de usuario y computador en otros dominios en el forest.
  + 1. Validación de la Instalación de ATA Gateway

Para validar que el ATA Gateway se haya instalado correctaente, se debe vertificar lo siguiente:

1. Revisar que el servicio ATA Gateway se esté ejecutando. Después de guarder las configuraciones de ATA Gateway, se podría tomar algunos minutos para que el servicio se inicie.
2. Si el servicio no se inicia, se debe revisar el archivo “Microsoft.Tri.Gateway-Errors.log” ubicado en la siguiente carpeta por defecto:   
   “%programfiles%\Microsoft Advanced Threat Analytics\Gateway\Logs”   
   Buscar las entradas con “transfer” o “service start.”
3. Revisar los siguientes contadores de rendimiento del ATA Gateway:
   1. **NetworkListener Captured Messages / sec**: Este contador sigue cuantos mensajes son capturados por el ATA por segundos. El valor debería ser desde quinientos a miles dependiendo del número de controladores de dominio que están siendo monitoreados y cuan ocupado está cada controlador de dominio. Valores de uno o dos dígitos pueden indicar un problema en la configuración de port mirroring.
   2. **EntityTransfer Activity Transfers/Sec**: Este valor debería estar en el rango de unos pocos cientos, cada pocos segundos.
4. Si este es el primer ATA Gateway instalado, después de unos pocos minutos, iniciar sesión en la consola ATA y abrir el panel de notificación en la parte derecha de la pantalla abierta. Se debería ver una lista de **Entities Recently Learned** en la barra de notificación sobre el costado derecho de la consola.
5. En la consola, buscar algo en la barra de búsqueda como por ejemplo un usuario o grupo en el dominio.
6. Abrir el Monitor de Rendimiento. En Performance tree, haga clic sobre **Performance Monitor** y luego haga clic en el signo más para **Add a Counter**. Expandir **Microsoft ATA Gateway** y bajar hasta **Network Listener Captured Messages per Second** y agregarlo. Luego, se debe asegurar que se vea actividad sobre el gráfico.

Figura 7: Performance Monitor – Agregar Contadores



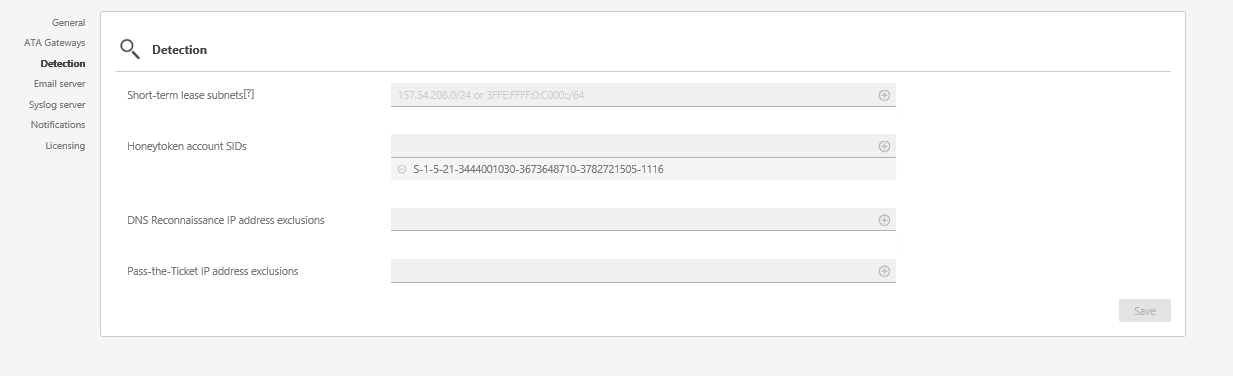
* 1. Paso 6: Configurar Subredes de Arriendo a Costo Plazo

Subredes de arriendo a corto plazo son subredes in las cuales la asignación de dirección IP cambian muy rápido, dentro de segundos o minutos. Por ejemplo, las direcciones IP usadas para las VPN o las redes inalámbricas.

Para ingresar la lista de las subredes de arriendo a corto plazo usadas en la organización, se deben seguir los siguientes pasos:

1. Desde la consola ATA sobre la máquina de ATA Gateway, haga clic en el icono de ajustes y seleccione **Configuration**.
2. Bajo **Detection**, ingrese las siguientes subredes de arriendo a corto plazo. Ingresarlas usalan el formato de notación con slash, por ejemplo: 192.168.0.0/24, y haga clic en el signo más.
3. Configurar exclusiones: Se pueden configurar direcciones IP para ser excluidas de las actividades sospechosas específicas.
   1. Paso 7: Configurar el Usuario Honeytoken
4. Desde la consola ATA sobre la máquina ATA Gateway, haga clic en la opción de ajustes y selecicone **Configuration**.
5. Bajo **Detection**, ingresar la información del usuario honeytoken:
   1. Para el SID de la cuenta honeytoken, ingrese el SID para la cuenta de usuario que no tendrá actividad de red, y haga clic en el signo más. Por ejemplo: S-1-5-21-72081277-1610778489-2625714895-10511.
   2. Para encontrar el SID para un usuario, ejecute el siguiente comando Windows PowerShell -> Get-ADUser UserName –Properties.

Figura 8: Configuración de Detección ATA



* 1. Paso 8: Información de Post-Instalación

Monitorear la línea de tiempo de ataques para ver actividades sospechosas detectadas, buscar usuario o computadores y ver sus perfiles.

Toma hasta 30 días para ATA construir perfiles de comportamiento para el ambiente. Así como ATA continúe aprendiendo del ambiente, este podría comenzar a detectar actividades de comportamiento sospechosas. Cada una de esas actividades deberían ser investigadas.

1. Apendice
   1. Configuración de Port Mirroring

La principal Fuente de datos que ATA usa viene de la inspección en profundidad del tráfico de red desde y hacia los controladores de dominio de Customer Name.

Para que ATA pueda ver el tráfico de red, el port mirroring necesita ser configurado. Port mirroring copia el tráfico sobre un puerto, conocido como el *puerto origen* a otro puerto, conocido como *puerto destino*. ATA trabaja con muchas soluciones que pueden espejar el tráfico, si el tráfico puede ser configurado como port mirroring a ATA, este puede ser usado para analizar amenazas a los sistemas. Para configurar port mirroring, revise la documentación que posea Customer Name del fabricante.

Los DC y ATA Gateways de Customer Name pueden ser Físicos o virtuales.

Los siguientes son los métodos comunes para port mirroring y algunas consideraciones. Customer Name necesita referirse a la documentación del producto del switch o servidor de virtualización para obtener información adicional. El fabriante deswitch podría utilizer diferente terminología.

* **Switched Port Analyzer (SPAN):** Copia el tráfico de red desde uno o más puertos del switch a otro puerto en el mismo switch. El ATA Gateway y los DC deben estar conectados al mismo switch físico.
* **Remote Switch Port Analyzer (RSPAN):** Permite a una organización monitorear el tráfico de red desde unos puertos origen distribuidos sobre múltiples switch físicos. RSPAN copia el tráfico de origen en una especial RSPAN-configured virtual LAN (VLAN). Esta VLAN necesita ser acoplada a los otros switch involucrados. RSPAN trabaja en capa 2.
* **Encapsulated Remote Switch Port Analyzer (ERSPAN):** Una tecnología propietaria de Cisco que trabaja en capa 3. Con ERSPAN, el usuario puede monitorear el tráfico a través de los switch sin la necesidad de trunks de VLAN. ERSPAN usa un ruteo de encapsulación genérico para copiar el tráfico de red monitoreado. ATA actualmente no puede recibir tráfico directo de ERSPAN. Para que ATA trabaje con tráfico ERSPAN, un switch o router que pueda desencapsular el tráfico necesita ser configurado como una destinación ERSPAN donde el tráfico es desencapsulado. El switch o router entonces necesita ser configurado para reenviar al ATA Gateway usando SPAN o RSPAN.
  + 1. Opciones soportadas de Port Mirroring

Tabla 16: Opciones de Port Mirroring

|  |  |  |
| --- | --- | --- |
| ATA Gateway | Domain controller | Considerations |
| Virtual | Virtual en el mismo host | El switch virtual necesita soportar port mirroring.  Mover una de las máquinas virtuales a otro host por sí mismo podría romper el port mirroring. |
| Virtual | Virtual en hosts diferentes | Se debe asegurar que el switch virtual soporta este escenario. |
| Virtual | Físico | Requiere un adaptador de red dedicado, de otra forma ATA verá todo el tráfico que venga desde el host y este tráfico será enviado al ATA Center. |
| Físico | Virtual | Se debe asegurar que el switch, sea físico o virtual, soporta port mirroring, basado en el siguiente escenario:   * Si el host virtual está en el mismo switch físico, se necesitará configurar en el switch el level span. * Si el host virtual está sobre un switch diferente, se necesitará configurar RSPAN o ERSPAN. \* |
| Físico | Físico en el mismo switch | El switch físico debe soportar SPAN/port mirroring. |
| Físico | Físico en un switch diferente | Requiere switch Físicos que soporten RSPAN o ERSPAN. \* |

\*ERSPAN esta solo soportado cuando la desencapsulación se realiza, de esta forma ATA analiza el tráfico.

* + 1. Hyper-V Virtual Switch – Windows Server 2012

Con port mirroring, el tráfico enviado desde o hacian un puerto de un Switch Virtual de Hype es copiado y enviado a un puerto espejado. Existe un rango de aplicaciones para port mirroring—existe un completo ecosistema de compañias de visibilidad de red que han diseñado productos para consumir port mirroring para administración de rendimiento, análisis de seguridad y diagnóstico de red. Con el port mirroring de Switch Virtuales de Hyper-V, se puede seleccionar los puertos del switch que son monitoreados como tambien los puertos que reciben copia del tráfico.

Los siguientes ejemplos muestran la configuración de port mirroring para que el tráfico que sea enviado y recibido por las máquinas MyVM y MyVM2 sea también enviado a la VM llamada MonitorVM.

Set-VMNetworkAdapter –VMName MyVM –PortMirroring Source

Set-VMNetworkAdapter –VMName MyVM2 –PortMirroring Source

Set-VMNetworkAdapter –VMName MonitorVM –PortMirroring Destination

También revisar <http://blogs.technet.com/b/networking/archive/2015/01/06/setting-up-port-mirroring-to-capture-mirrored-traffic-on-a-hyper-v-virtual-machine.aspx>

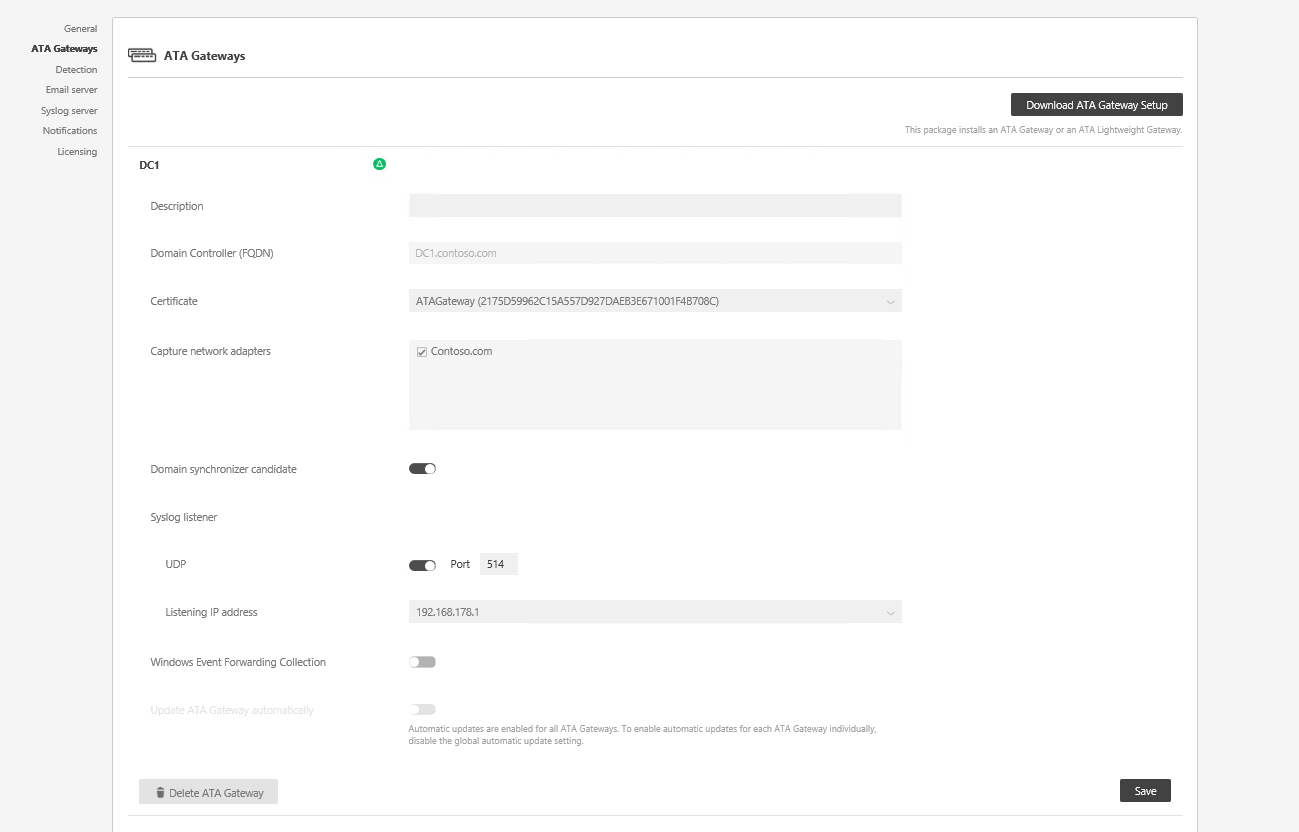
* 1. Configuring Security Information and Event Management (SIEM) Integration

To enhance ATA detection of Pass the Hash (PtH), ATA needs Windows Event log ID 4776. This can be forwarded to the ATA Gateway in one of two ways—by configuring the ATA Gateway to listen for SIEM events or by using Windows Event Forwarding (WEF).

* + 1. Configuración del ATA Gateway para escuchar y aceptar eventos del SIEM

1. Sobre la configuración del ATA Gateway, activar **Syslog Listener UDP**.

Configurar la Listening IP Address como se describe en la siguiente figura. El puerto por defecto es 514.



Customer Name necesita configurar su SIEM o servidor Syslog para reenviar el Windows Event ID 4776 a la dirección IP seleccionada en la figura previa. Para información adicional sobre la configuración del SIEM, refierase a la ayuda técnica en línea de SIEM o a las opciones de soporte para requerimientos de formato específico para cada servidor SIEM.

* + 1. Soluciones SIEM Soportadas

Para ver las soluciones SIEM soportadas, ver <https://technet.microsoft.com/en-us/library/dn707705.aspx>.

* 1. Configuración de Windows Event Forwarding (WEF)

Si Customer Name no tiene un servidor SIEM, el administrador puede configurar los controladores de dominio de Customer Name para reenviar el Windows Event ID 4776 directamente a uno de los ATA Gateways.

**NOTA:** Los mismos pasos deben ser completados para los ATA Lightweight Gateway.

La siguiente sección es informativa y está fuera del alcance de este proyecto.

1. Sobre la configuración del ATA Gateway, activar **Windows Event Forwarding Collection**.
2. Cuando el administrador active este ajuste, el ATA Gateway buscará en los Forwarded Events log por Windows Events que hayan sido reenviados a él desde los controladores de dominio.
3. Configurar los controladores de dominio para reenviar el Windows Event ID 4776 a los ATA Gateways. Para información adicional sobre Windows Event Forwarding, ver [Configure Computers to Forward and Collect Events](https://technet.microsoft.com/en-us/library/cc748890).