# Iniciar sesión en un escritorio remoto mediante RDP cambia el usuario asociado a una dirección IP

## Contenido



## Introducción

Si inicia sesión en un host remoto mediante Remote Desktop Protocol (RDP), y el nombre de usuario remoto es diferente al de su usuario, el sistema FireSIGHT cambia la dirección IP del usuario asociado a su dirección IP en FireSIGHT Management Center. Provoca cambios en los permisos del usuario en relación con las reglas de control de acceso. Se dará cuenta de queEl usuario incorrecto está asociado con la estación de trabajo. Este documento proporciona una solución para este problema.

## Prerequisites

Cisco recomienda tener conocimientos sobre el sistema FireSIGHT y el agente de usuario.

> **Nota**: La información de este documento se creó a partir de los dispositivos de un entorno de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

## Causa raíz

Este problema se produce debido a la forma en que Microsoft Active Directory (AD) registra los intentos de autenticación RDP en los registros de seguridad de Windows del controlador de dominio. AD registra el intento de autenticación para la sesión RDP contra la dirección IP del host

de origen en lugar del punto final RDP al que se está conectando. Si inicia sesión en el host remoto con una cuenta de usuario diferente, cambiará el usuario asociado con la dirección IP de la estación de trabajo original.

# Verificación

Para comprobar que esto es lo que está sucediendo, puede comprobar que la dirección IP del evento de inicio de sesión de la estación de trabajo original y el host remoto RDP tienen la misma dirección IP.

Para buscar estos eventos, deberá seguir los pasos que se indican a continuación:

Paso 1: Determine el controlador de dominio con el que se autentica el host:

Ejecute el siguiente comando:

```
nltest /dsgetdc:<windows.domain.name>
```

Ejemplo de salida:

```
C:\Users\WinXP.LAB>nltest /dsgetdc:support.lab
DC: \\Win2k8.support.lab
Address: \\192.X.X.X
Dom Guid: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Dom Name: support.lab
Forest Name: support.lab
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST
CLOSE_SITE FULL_SECRET WS 0x4000
The command completed successfully
```

La línea que inicia "DC:" será el nombre del controlador de dominio y la línea que inicia "Address:" será la dirección IP.

Paso 2: Uso del registro RDP en el controlador de dominio identificado en el paso 1

Paso 3: Vaya a **Inicio > Herramientas administrativas > Visor de eventos**.

Paso 4: Profundice en **Registros de Windows > Seguridad**.

Paso 5: Filtre por la dirección IP de su estación de trabajo haciendo clic en Filtrar registro actual, haciendo clic en la ficha XML y haciendo clic en editar consulta.

Paso 6: Introduzca la siguiente consulta XML, sustituyendo **<ip address>** por su dirección IP

```
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">
*[EventData[Data[@Name='IpAddress'] and(Data='<IP address>')]]
</Select>
</Query>
</QueryList>
```

Paso 7: Haga clic en el **Evento de Inicio de Sesión** y haga clic en la pestaña **Detalles**.

Un ejemplo de resultado:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing"
Guid="{XXXXXXXX-XXX-XXXX-XXX-XXXXXXXXXXXX}"/>
<EventID>4624</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2014-07-22T20:35:12.750Z" />
<EventRecordID>4130857</EventRecordID>
<Correlation />
<Execution ProcessID="576" ThreadID="704" />
<Channel>Security</Channel>
<Computer>WIN2k8.Support.lab</Computer>
<Security />
</System>
- <EventData>
<Data Name="SubjectUserSid">S-1-0-0</Data>
<Data Name="SubjectUserName">-</Data>
<Data Name="SubjectDomainName">-</Data>
<Data Name="SubjectLogonId">0x0</Data>
<Data Name="TargetUserSid">S-X-X-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXX-XXXX</Data>
<Data Name="TargetUserName">WINXP-SUPLAB$</Data>
<Data Name="TargetDomainName">SUPPORT</Data>
<Data Name="TargetLogonId">0x13c4101f</Data>
<Data Name="LogonType">3</Data>
<Data Name="LogonProcessName">Kerberos</Data>
<Data Name="AuthenticationPackageName">Kerberos</Data>
<Data Name="WorkstationName" />
<Data Name="LogonGuid">{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x0</Data>
<Data Name="ProcessName">-</Data>
<Data Name="IpAddress">192.0.2.10</Data>
<Data Name="IpPort">2401</Data>
</EventData>
```

Complete estos mismos pasos después de iniciar sesión mediante RDP y observará que recibirá otro evento de inicio de sesión (Event ID 4624) con la misma dirección IP que se muestra en la línea siguiente de los datos XML del evento de inicio de sesión del inicio de sesión original:

```
<Data Name="IpAddress">192.x.x.x</Data>
```

# Solución

Para mitigar este problema, si utiliza el Agente de usuario 2.1 o superior, puede excluir cualquier cuenta que desee
se utiliza principalmente para RDP en la configuración del agente de usuario.

Paso 1: Inicie sesión en el host del agente de usuario.

Paso 2: Inicie la interfaz de usuario del agente de usuario.

Paso 3: Haga clic en la pestaña **Excluded Usernames**.

Paso 4: Introduzca todos los nombres de usuario que desea excluir.

Paso 5: Haga clic en **Guardar**.

Los usuarios incluidos en esta lista no generan eventos de inicio de sesión en FireSIGHT Management Center y no se pueden
asociados a direcciones IP.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).