Create a Remote Log Source - Wincollect.mobile.phone

Create a Remote Log Source (Wincollect)

Topics Discussed

To obtain Log Relay and to configure your account for remote log collection, you must have the following AMP permissions added to your account:

- Write Virtual Machine
- Delete Log Management
- Read Log Endpoints
- Read Log Relays
- Write Log Relays
- Delete Log Relays

You can use this document to add a remote log collector to a Wincollect remote device (log source).

Pre-Deployment Considerations

Before you begin, review the following requirements:

Log Relay

For remote log collection, you must have **Log Relay** added to your account.

- To learn how to add **Log Relay** to your account, see Obtain Log Relay for Remote Log Collection.

Create A Remote Log Source

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.
3. Click **External Sources**.
4. Click the plus (+) sign.
    - If you do not have any log sources already created, then click **Add a New Log Source**.
5. Complete the missing fields:
    - In **Endpoint**, select the available Armor Endpoint.
    - In **Log Source Type**, select **Microsoft Windows Security Event Log**.
    - In **Hostname**, enter the system hostname that matches the system for log collection.
        - The hostname is case-sensitive and must match the exact same letters casing as the logs that are sent into this log source.
    - In **Protocol**, based on your selection in **Log Source Type**, select the available protocol.
6. Click **Save Log Source**.
7. In the **Sources** screen, refresh the screen until the log source reaches an **Online** status.

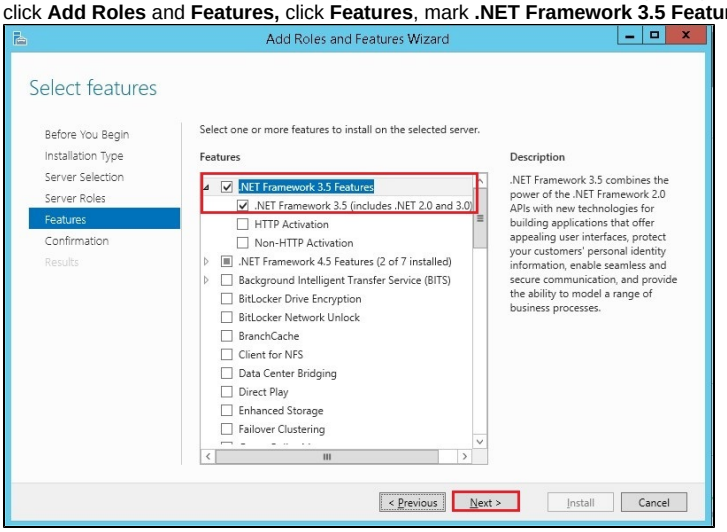
Update Access Control List

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
2. Click **Log & Data Management**.

3. Click **External Sources**.
4. Hover over the gear icon, and then click the blue icon for **Edit Access Control List**.
5. In the field, enter a public IP address or a range of addresses that will send data to Armor. Enter the address in CIDR notation.
6. Click **Add CIDR**.
7. Click **Save ACL**.

Install and Configure Wincollect to Forward Windows Security Logs

1. Download and install two Wincollect installers.
    - Download a standard installer (x86 o x64):
        - https://get.core.armor.com/logging/wincollect/7.2.8/wincollect.exe
    - Download a standalone patch installer:
        - https://get.core.armor.com/logging/wincollect/7.2.8/wincollect-standalone-patch-installer.exe
2. Log into your server.
3. Right-click the **Wincollect Standard Installe**r, and then select **Run as administrator**.
    - Click **Next** until you reach the **Setup Type** screen.
    - In the **Setup Type** screen, select **Stand Alone**.
    - Click **Next** until you see the option to install. Click **Install**.
    - After the installation is complete, click **Finish** to close the window.
4. Right-click the **Wincollect Standalone Patch Installer**, and then select **Run as administrator**.
    - Click **Next** until you reach the **Custom Setup** screen.
    - Verify that **Configuration Console** is set to install on the local hard drive.
    - Click **Next** until you see the option to install. Click **Install**.
    - Click **Finish** to close the window.
5. Install .Net 3.5.
    - If you already have .NET 3.5 installed, then you can skip this step.
    - For Windows Server 2012 and higher, you can access the **Server Manager** to perform the installation. (In the top menu, click **Manager**, click **Add Roles** and **Features,** click **Features**, mark **.NET Framework 3.5 Features**, mark **.NET Framework 3.5**, and then click **Next**.)



Download A TLS Certificate

This step only applies to users who currently have TLS certificates. If you have not previously configured your account for TLS certificates, then you can skip to **Step 5: Configure your Wincollect Configuration Console**.

1. Download your unique TLS certificate from Armor.
2. Copy the following code into a local server file, and then name the file **Get-RemoteSSLCertificate.ps1**.

```
[CmdletBinding()]
param (
  [Parameter(Mandatory = $true)]
  [string]
  $ComputerName,

  [int]
  $Port = 443
)

$Certificate = $null
$TcpClient = New-Object -TypeName System.Net.Sockets.TcpClient
try {

  Write-Verbose ("Attempting to download certificate from {0}:{1}" -f $ComputerName, $Port)
  $TcpClient.Connect($ComputerName, $Port)
  $TcpStream = $TcpClient.GetStream()

  $Callback = { param($sender, $cert, $chain, $errors) return $true }

  $SslStream = New-Object -TypeName System.Net.Security.SslStream -ArgumentList @($TcpStream, $true,
$Callback)
  try {

    $SslStream.AuthenticateAsClient('', $null, "Tls12", $false)
    $Certificate = $SslStream.RemoteCertificate

  }
  finally {
    $SslStream.Dispose()
  }

}
catch {
  Write-Error ("Unable to download certificate from {0} on port {1}.`nPlease validate that these are
correctly configured in `$env:logEndpoint and `$env:logPort to match the information provided from
https://portal.armor.com/" -f $ComputerName, $Port)
}
finally {
  $TcpClient.Dispose()
}

if ($Certificate) {
  Write-Verbose ("Certificate downloaded from {0}:{1}" -f $ComputerName, $Port)
  Write-Verbose ("Validating certificate from {0}:{1}" -f $ComputerName, $Port)
  if ($Certificate -isnot [System.Security.Cryptography.X509Certificates.X509Certificate2]) {
    $Certificate = [Convert]::ToBase64String((New-Object -TypeName System.Security.Cryptography.
X509Certificates.X509Certificate2 -ArgumentList $Certificate).RawData, "InsertLineBreaks")
    $Certificate = "{0}`n{1}`n{2}" -f "-----BEGIN CERTIFICATE-----", $Certificate, "-----END
CERTIFICATE-----"
    Write-Verbose ("Validated certificate from {0}:{1}" -f $ComputerName, $Port)
  }

  Write-Output $Certificate
}
else {
  Write-Error ("Empty certificate downloaded from {0} on port {1}.`nPlease validate that these are
correctly configured in `$env:logEndpoint and `$env:logPort to match the information provided from
https://portal.armor.com/" -f $ComputerName, $Port)
}
```

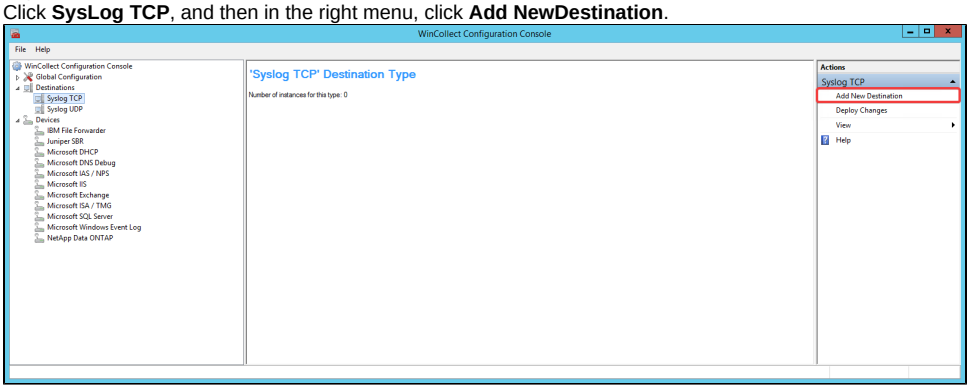
3. In a PowerShell window, navigate to the folder that contains your newly created .ps1 file.
4. Run the following script:

```
.\Get-RemoteSSLCertificate.ps1 -ComputerName <Armor Provided Endpoint FQDN> -Port <Armor Provided Port
Number>
```

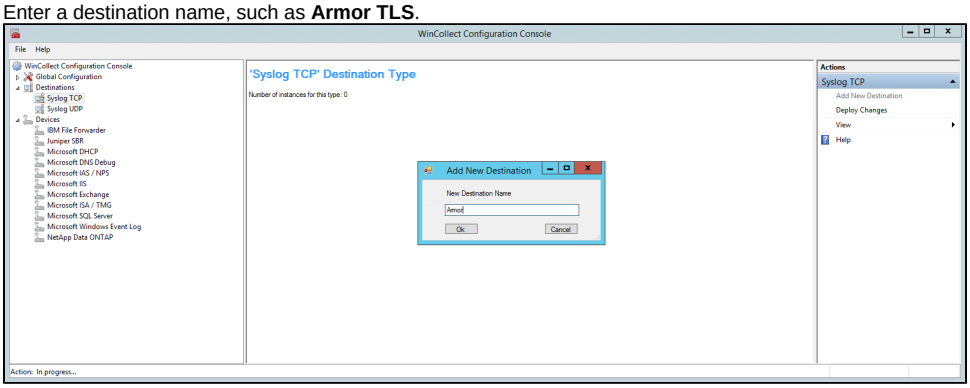
5. Copy the certificate into a new file to save for later use.

Configure Your Wincollect Configuration Console

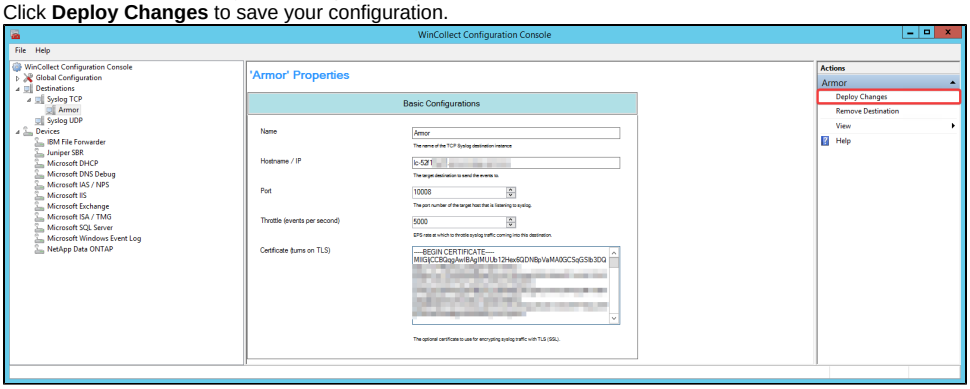
1. In your machine, open the **Wincollect Configuration Console**
2. Expand **Destinations**.
3. Click **SysLog TCP**, and then in the right menu, click **Add NewDestination**.



4. Enter a destination name, such as **Armor TLS**.

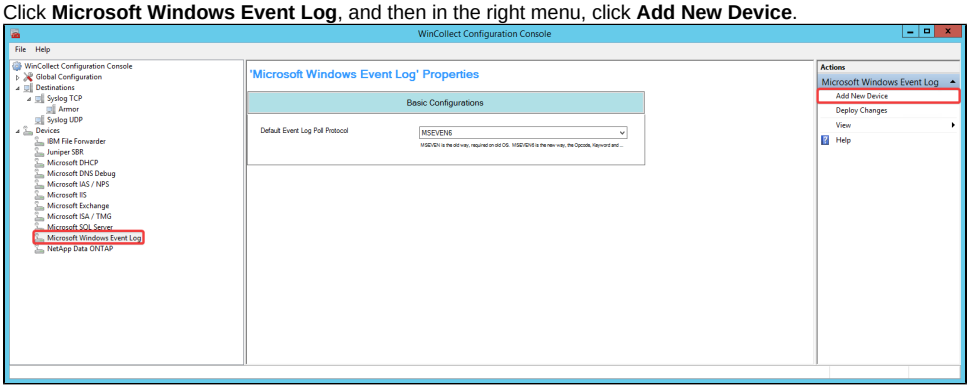


5. Expand **SysLogTCP**, and then click the newly created destination name to open the destination configuration menu.
    - In **Hostname**, enter the Armor-provided endpoint FQDN for your source.
    - In **Port**, enter the Armor-provided port number for your source.
    - In **Certificate**, enter the newly created certificate.
        - This step only applies to users who currently have TLS certificates. If you have not previously configured your account for TLS certificates, then you can skip this step.
    - Click **Deploy Changes** to save your configuration.



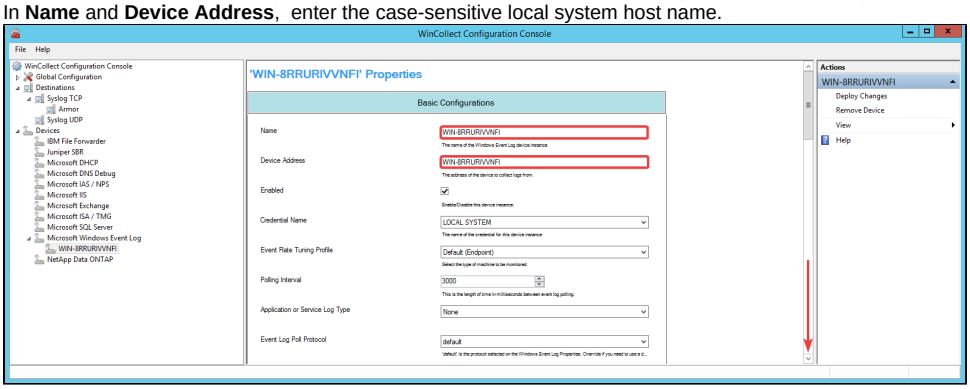
6. Expand **Devices**.

7. Click **Microsoft Windows Event Log**, and then in the right menu, click **Add New Device**.

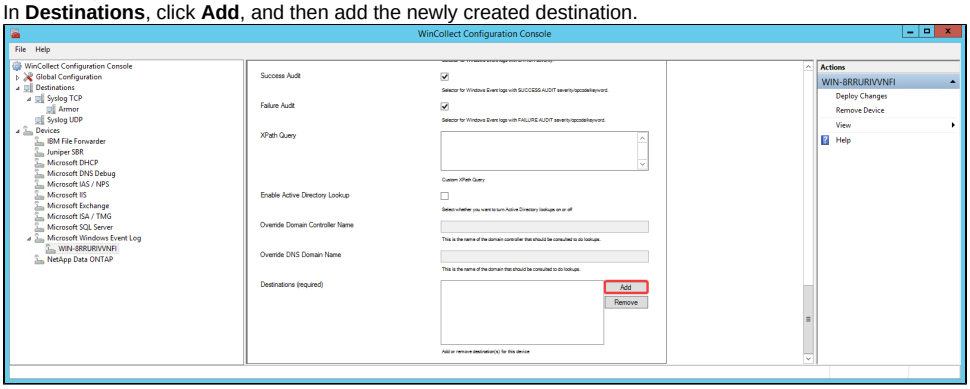


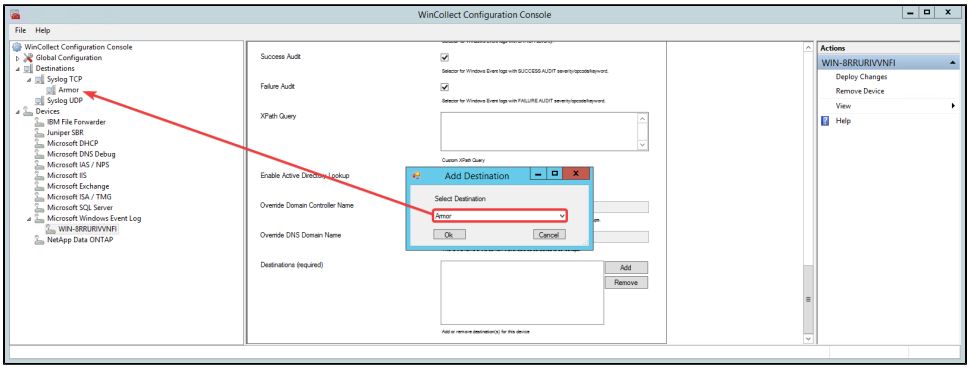
- Enter a device name. (Armor recommends that you use the case-sensitive server name.)

8. Expand **Microsoft Windows Event Log**, and then click the newly created device to open the device configuration menu.
   - In **Name** and **Device Address**, enter the case-sensitive local system host name.

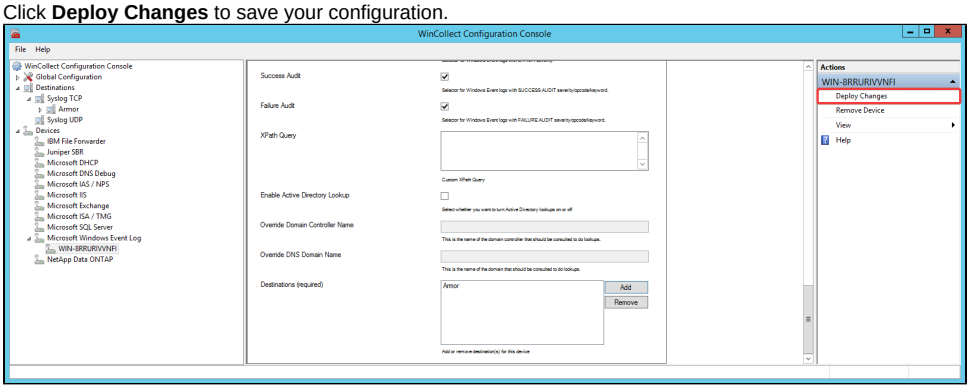


   - In **Security**, verify that the box is checked.
   - In **Destinations**, click **Add**, and then add the newly created destination.





- Click **Deploy Changes** to save your configuration.



Verify Configurations

1. Log out of the server, and then log back in.
    - This action will generate a log which you can use to verify that the configuration to Armor was successful.
2. In the Armor Management Portal (AMP), in the left-side navigation, click **Security**.
3. Click **Log & Data Management**.
4. Click **Search**.
5. In the search field, enter the name of your server to locate the newly generated log.
    - You may need to refresh the screen to see new logs.