App I On-Demand Agentless Captures (Experimental)

You can perform on-demand agentless captures directly on supported devices and operating systems that support tcpdump using a secure SSH connection.

Note—To perform on-demand agentless captures, you must have one of the following sets of licences:
• AppTransaction Xpert Plus
• AppTransaction Xpert Module with AppTransaction Xpert Advanced Capabilities

---

Currently, the following devices and operating systems are supported:

- Device
  - — F5 BIG-IP
- UNIX-based operating systems
  - — Linux
  - — Solaris SPARC
  - — Solaris Intel/AMD

This functionality makes no changes to the device/machine and stores no local data on the device (except the tcpdump data file, which is downloaded to the Capture Manager and immediately deleted from the device/machine as soon as you finish the capture).

Note—The on-demand agentless capture feature is included as an experimental feature in AppTransaction Xpert. During this phase, customers can use this feature “as-is” while OPNET evaluates whether to include this or similar functionality in future releases.

If you encounter any issues while using this feature, contact Technical Support. However, because the feature is experimental, OPNET may not provide solutions for all reported problems.

This section has the following subsections:

- Important Notes
- Workflow Description
- Configuring On-Demand Agentless Captures

Important Notes

When performing an on-demand agentless capture, note the following:

- You can run on-demand captures only; continuous captures are not supported.
- This feature is designed for capturing on F5 devices and UNIX machines that have both tcpdump and SSH functionality.
- SSH (Secure Shell) must be enabled on the device/machine.
- You must have a valid username/password for each device/machine on which you want to capture. Additionally, you must have permission to run tcpdump.
- The first time you connect to a device/machine in the current AppTransaction Xpert session, you must enter a valid username/password for that device. (You can choose to retain the usernames/passwords for the current session, but AppTransaction Xpert does not save the login information to disk.)
- You cannot store packet traces on the device/machine. When you finish a capture, Capture Manager downloads all capture data from all devices/machines.
- Because tcpdump copies packets to disk, you must configure the agent so that a capture does not consume all available disk space on the device/machine. The Filter, Maximum size of packet data to capture (bytes), and Maximum number of packets to capture options are especially relevant for limiting packet trace sizes.

  For more information, see Configuring On-Demand Agentless Captures.
- You must set the “path.dumps” attribute(s) in the respective configuration file to match your default directory after an SSH login. If the “path.dumps” attribute is not set properly, then the file cannot be downloaded after a capture.

  The location and names of the configuration files are:

  — F5 BIG-IP: <*install_dir*>\sys\configs\ace_capture_f5.capcfg

  — UNIX: <*install_dir*>\sys\configs\ace_capture_unix.capcfg

  Note that in the UNIX configuration file, there is a section for each supported operating system (e.g., “start_linux”, “start_solaris_sparc”, “start_solaris_intel”).

  After editing the .capcfg file, you must restart AppTransaction Xpert for the changes to take effect.
- For information about the required user privileges on UNIX platforms, see FAQ 2360 on the Support Website.

Workflow Description

The following procedure describes how to perform an on-demand agentless capture on an F5 BIG-IP device or on a UNIX machine.

Procedure I-1 Capturing Traffic on an F5 BIG-IP Device or a UNIX Machine

1. Verify that you have a valid username and password on the device/machine.
2. Open Capture Manager and click the On-Demand tab.
3. Create an agent list for the device/machine if you have not already done so:

   For each interface on which you want to capture, do the following:

   3.1 Click Add Agent… to open the Remote Application Capture Agent Editor (Figure I-1).

   3.2 Select the Capture Agent Type. Choose one of the following:

   - F5 BIG-IP
   - UNIX (no installed agent)

   3.3 Specify settings for the agent. (You might be prompted for a username and password before you can access the device.)

   For descriptions of these settings, see Table I-1.

   3.4 Repeat step 3.1 through step 3.3 for every interface on which you want to capture.

   3.5 (*Optional*) Save the complete agent list by clicking Save Agent List…
4. Verify that all agents are enabled (checked) in the Capture Manager treeview, then click Start Capture.

   If prompted, enter your login username and password for that device.

   Note—AppTransaction Xpert retains your username and password for the current session but does not save this information. Therefore, you must supply your username/password before the first capture in the current session of AppTransaction Xpert.
5. Run the application transaction that you want to capture.
6. When the transaction finishes, click Stop Capture.

   ➥ AppTransaction Xpert downloads the packet traces from all interfaces automatically.

End of Procedure I-1

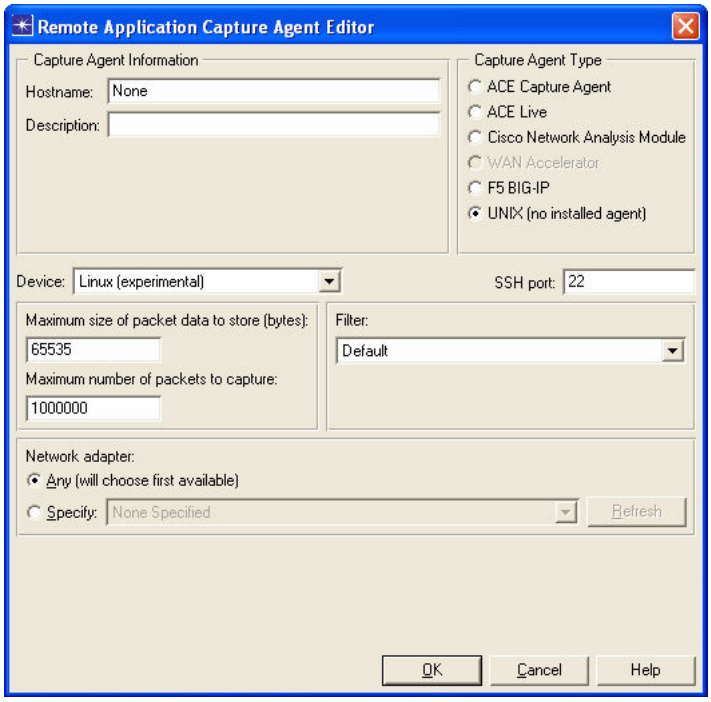
Configuring On-Demand Agentless Captures

The Remote Application Capture Agent Editor has some options that are especially relevant to F5 devices. These options are described in Table I-1 on page ATX-I-5.

WARNING—You must limit packet trace sizes or you might run out of disk space.

Because tcpdump creates a separate copy of each captured packet, you must take care not to consume more disk space than is necessary on the F5 device. The Filter, Maximum size of packet data to capture (bytes), and Maximum number of packets to capture options are especially relevant for limiting packet trace sizes.

Figure I-1 Remote Application Capture Agent Editor (F5 Devices and UNIX Machines)



The following table lists the configuration options available in the Remote Application Capture Agent Editor.

Table I-1 Remote Application Capture Agent Editor Options (F5 Devices and UNIX Machines)

Option	Description
Hostname	Hostname or IP address of the device/machine.
Description	Description that appears in the Capture Manager treeview.
Capture Agent Type	For F5 BIG-IP device, select “F5 BIG-IP”. For UNIX machines, select “UNIX (no installed agent)”.
Device	For F5 BIG-IP, select “F5 BIG-IP”. For UNIX, select one of the following: - Linux - Solaris SPARC - Solaris Intel/AMD
SSH port	The default SSH port is 22. Change this setting only if the device/machine uses a different port for SSH connections.
Maximum size of packet data to capture (bytes)	Limits the amount of data in each packet. However, note the following: • If your network uses any form of IP tunneling that encapsulates IP packets, do not specify a value that is less than 130 bytes per packet. This is necessary to ensure that all protocol header data is captured. • If you limit the number of bytes captured per packet, and application payload data is not captured, you might be unable to perform detailed application-layer analyses after importing the traffic into AppTransaction Xpert.
Maximum number of packets to capture	You might want to specify a lower value than the default.
Filter	Select the packet filter to use with the capture, or edit a custom filter by choosing Edit or Manually Edit.
Network adapter	Always select a specific interface on the device. (Do not select “Any”.)