



Locate Frequently Asked Questions

1. What is Locate?

Locate is a network appliance that combines information from three sources in real-time to create a comprehensive view of who is using which IP address on your network and where they're connected to your switched network infrastructure—which switch port they're on. Since Locate is able to identify who is using an IP address and MAC address and it has access to your staff directory, it can determine the location (office or cube) and phone number for the IP address. This is critical for tracking down problem IP addresses. This information is available in real-time through an easy-to-use web application. Additional collection nodes—or sensors (also an appliance) are available for distributed enterprise networks. This is explained in more detail in the “How does Locate work?” section.

2. How does Locate work?

Locate works by correlating the activity of people on your network with your directory information and the information on your switched network. Locate includes the following subsystems:

Sniffer – The sniffer inspects network packets for person identifying information. This information is contained in authentication and messaging traffic.

Crawler – The crawler periodically scans the switched network to identify which computer is connected to which switch port.

A/D – LDAP – The Locate system periodically pulls directory information from your directory stores.

Application – The Locate application correlates all this information and makes it available in a web application. The information is fully searchable and exportable.

3. Where do I connect Locate?

The primary server has two network connections. One connection is the sniffer port and the other port is the connection to the web-based management application. The management port is connected to your network like a standard server or workstation and is assigned a static IP address through the front panel. You access the web application from this IP address. The sniffer port is connected to a switch port that contains your mirrored authentication traffic (A/D server). If you're not running AD, you connect the sniffer port to a switch port that contains your mirrored Internet traffic. Additional collection nodes are available to collect traffic from distributed A/D servers or multiple Internet Gateways. Collection nodes sync their data with the primary Locate server so all information is available through the Locate web application.

4. When do I need to use a collection node (sensor)?

If you're using multiple Microsoft Active Directory servers across the enterprise, you need collection nodes at each point of authentication. Connection nodes can also be deployed at the Internet Gateway to collect identifying information from Internet traffic.

5. Is Locate easy to install?

Setting up a Locate appliance requires some basic configuration information such as an IP Address, Subnet Mask, Gateway, and Nameserver. The unit also has two physical ports, a Gig-E management port and a Gig-E sniffer port, for detecting network traffic.



Locate also requires information from two sources: Information about your people typically found in an Active Directory or LDAP server and information about the managed switches on your network, which can be loaded using a CSV file.

After it is configured, the Locate appliance immediately begins the IP-to-People mapping by examining network traffic off the wire and pulling information from the managed switches on the network.

6. Once configured, how does Locate stay up to date with the latest information about my people and switches?

The Locate system periodically pulls directory information from your directory stores and the crawler within Locate periodically scans the switched network to identify which computer is connected to which switch port.

7. Where do I install the Locate appliance?

On networks that use Active Directory to authenticate, connect the Locate appliance into the spanned or mirrored port on the switch (or into any port on a shared media hub) that can see Active Directory/LDAP/Exchange traffic.

For networks that use Sendmail, the Locate appliance connects to the Internet Gateway.

8. What if I have multiple points of authentication?

You need a collection node at each point of authentication or the installation of the A/D server collection software.

9. What switch makes/models does Locate support?

Currently, all of Locate's features are supported on switches that have all of the following features:

- RFC compliant SNMP Version 2 MIB
- RFC-1493 compliant BRIDGE-MIB
- Port mirroring feature (such as SPAN)

If your current switch does not support the above features, check the Matrix below to determine what features are available from Locate.

Switch Capability/Locate Feature Matrix

	SNMPv2 + RFC1493	?+ SNMPv2 - RFC1493	?- SNMPv2 - RFC1493
Map People Layer (person to IP)	yes	yes	yes
Map Network Layer (IP to MAC)	yes	yes	yes (except statically assigned)

			addresses)
Map Physical Layer (MAC to Switch Port)	yes	no	no
“Motion Detector”	yes	yes (except Physical Layer)	yes (except Physical Layer)
“Isolator”	yes	no	no
“Instant Assist”	yes	yes	yes
“LDAP Integration”	yes	yes	yes

10. I don't have any extra span or mirrored ports, can I still use Locate?

Yes. Locate can capture authentication events if the A/D server collection software is installed on the Active Directories.

11. Will Locate impact my network or switch performance?

The impact of the sniffer functionality is minimal and is equivalent to any other device that uses mirrored traffic. The impact of the crawler functionality is also minimal, and although it crawls your selected switches once every 15 minutes, it only pulls a very small subset of the switch information using SNMP.

12. How can I integrate the information captured in Locate with other systems?

By using Locate's web services, you can integrate the information captured in Locate with other systems.

13. We use something other than Remote Desktop, eg . Altiris, does Locate support other tools?

Locate currently only supports Remote Desktop.

14. Do any 3^d party interfaces exist? Eg. OpenView, ArcSite, etc.

Not currently.

15. I have remote users who VPN into the corporate network, does Locate identify them?

Locate can identify remote users who VPN into the corporate network.

16. How many collection nodes can a Primary Server support?

The Locate appliance can be configured to address an unlimited number of collection nodes. Collection nodes are deployed when there are multiple points of authentication on an Active Directory network.



17. Will collection nodes use a lot of bandwidth communicating with the Primary Server?

Each collection node uses minimal bandwidth when communicating with the Primary Server.

The amount of node communication is not only related to the number of active workstations/users at the location of each node, but also to the number of changes occurring on the network at the location. Nodes only communicate deltas in the layer mappings, i.e. changes in the internal mappings tables.

Note: When initially connected, everything is a “delta,” however as time progresses, the majority of data collected by Locate simply verifies already determined mappings, and is therefore not communicated to other nodes.

18. Will installing the A/D server collection software have an impact on my A/D server’s performance?

The eTelemetry Active Directory Collection Software is a small, low-impact, .NET Windows Service that is installed on Windows Server domain controllers. When a user or machine authenticates to Active Directory, the eTelemetry Active Directory Collection Software forwards the authentication information (user account, machine account, IP address) to Locate. As a passive service, it only runs and consumes CPU cycles when a security event occurs. The eTelemetry Active Directory Collection Software is a free alternative to deploying a Locate Collection Node.

19. We have a mix of Windows PCs, MACs, Linux, and Unix Systems on our network, will Locate map all of them?

Yes.

Given a compatible switched environment, Locate can map the Physical and Network Layer for all PCs, Macs, Linux, Unix, and any other device using TCP/IP on the network.

Locate maps the People Layer for any device authenticating to a central authentication point. Windows and Mac OS X natively support all of Microsoft’s Active Directory Services. Linux and Unix System also support authentication to the Active Directory Service.

If central authentication is not deployed or available, Locate is typically installed at the Internet Gateway. At this location, Locate maps the People Layer by inspecting Internet Protocols, which are uniform across all platforms (from Locate’s perspective).

20. Does eTelemetry offer maintenance plans?

Annual maintenance is available for purchase. The maintenance plan for eTelemetry’s products includes:

- The most current release and version of the product, bug fixes, or patches
- New releases or versions during the annual maintenance period
- Hardware maintenance
- Customer support via e-mail and phone 9:00 a.m. to 5:00 p.m. Eastern Standard Time, excluding holidays.



21. How long does Locate store the historical information?

Locate stores and allows the user to query information covering the previous 5 years.

22. What if my Locate appliance is damaged?

Call or e-mail our Product Support Center.