IS&T Policies: DHCP Usage Logs Policy

On this page:

Policy

IS&T records a variety of information about both the operation and/or use of its network services. When used in conjunction with IS&T's Host Registration database, records contained in logs showing the use of dynamic IP addresses on MITnet allow IS&T staff to follow up on problems, incidents, and inquiries.

These logs are retained for 30 days after their creation date. All of these logs are considered confidential, and as such IS&T takes active measures to prevent unauthorized access during the retention period.

Circumstances may arise where a log, or more usually a very small subset of one day's log, may need to be kept for longer than 30 days and, potentially, disclosed to certain third parties. The use of any such retained information by authorized staff, and the release of any log information to third parties, are done under the direction and with the approval of MIT's Office of the General Counsel.

This IS&T policy is limited to the Dynamic Host Configuration Protocol (DHCP) services and logs created in connection with MITnet. It does not apply to DHCP services or logs created by other Departments, Labs & Centers (DLCs) at MIT. IS&T recommends that other IT groups at MIT create similar policies that are based on business practices and are consistent with the needs and desires of those DLCs.

Rationale

This policy implements MIT's Privacy Policy specifically for the collection and retention of DHCP logs. In setting the retention period, IS&T has weighed a variety of competing interests, chiefly the need to maintain robust operational reliability of MIT's network, the need to be responsive to third parties who report issues that we need to investigate or resolve, and the desire to limit log retention to reduce opportunities for inadvertent disclosure of operational data.

Implementation

The DHCP server is configured to provide dynamic addresses automatically as needed. The logs of information are maintained on an IS&T-managed server. Each log is tagged with its creation date; once a day, the system deletes logs that are 30 days old.

When any network device, e.g., a computer, connects to MITnet and is assigned a dynamic IP address, MIT's DHCP server adds a record to its log containing the following information:

- The date and time of the request
- The MAC address of the requesting device or computer
- The IP address provided
- The specific DHCP command that was issued
- Other technical information related to the request

In the event of a request relating to a potential legal proceeding, IS&T staff may create a case in Request Tracker and store subsets of a log pertinent to the case at hand in the case record.

The DHCP server is in a secure location and complies with secure data storage best practices. IS&T's Network Services Infrastructure team acts as the data custodian for DHCP logs, and ensures that the logs are stored securely and are deleted when they expire.

The DHCP logs capture only one type of network usage. Related, but not addressed in this policy, are Virtual Private Network (VPN) usage logs, hostnames/static IP addresses usage logs, or dialup usage logs, among others.

Implications

Retaining and securing DHCP usage logs as described above are necessary to ensure that the confidentiality of the DHCP lease logs is protected but that the information in the logs is still available as needed to ensure MITnet's security and integrity.

MIT is required to comply with a court order or valid subpoena that requests the disclosure of information contained in DHCP logs. Failure to comply could have serious consequences for the individuals, IS&T, and the Institute. MIT's Office of the General Counsel is qualified and authorized to confirm that a request for information contained in logs is legitimate and not an improper attempt to gain access to confidential information.

Glossary

DHCP: Dynamic Host Configuration Protocol. This protocol defines the process by which a device can dynamically receive an IP address from a pool of addresses, instead of requiring the device to have a fixed IP address. This is ideal for devices like laptops, which will not all be connected to the network at all times from the same location.

Dynamic IP Address: When a device has not been assigned a Static IP address, an Internet service provider will assign an address at the time the device is connecting to the Internet.

IP Address: Internet Protocol (IP) Address. See references below for more information on network addressing.

DLCs: A collective term meant to describe the common elements among MIT's many academic, administrative and research units, while acknowledging the many differences amongst MIT units.

Static IP Address: A number (in the form of a dotted quad) that is assigned to a network device or computer by an Internet service provider (ISP) which will be its permanent address on the Internet.

VPN: Virtual Private Network. A technology that in MIT's usage facilitates secure communications from remote locations to a known location at MIT, typically over the public Internet. However, VPNs are not inherently about security or performance, but rather that they provide a "tunnel" on top of some other network in support of a given customer or client community.

History

Status: In effect

Policy Steward: Paul Acosta

Policy Owner: Marilyn T. Smith

RELATED PAGES AND HOW TO

IT Policies

Virtual Private Network (VPN)

MITnet Bootstrap Registration

MIT Privacy and Disclosure of Information Policy

ABOUT IS&T

NEWS

OUR ORGANIZATION

MISSION & STRATEGIC PLAN

IT POLICIES

IT GOVERNANCE

JOB OPENINGS

Massachusetts Institute of Technology

Information Services and Technology | 617.253.1101
Ask the Help Desk or contact the IS&T Webmasters.

FOR FACULTY & STAFF

FOR STUDENTS

FOR VISITORS

FOR IS&T STAFF

FOLLOW US