Setting the Xerox Secure Access Unified ID System® Authentication Device IP Address

White Paper

Version 1.5: June 2009

Contents

Contents

Setting the Xerox Secure Access Unified ID System Authentication Device IP Address

This chapter includes:

1. Purpose

This document is a summary of the bootp process for a terminal configure to run in mode 2 (Office Environment) Correct IP Address assignment is essential to ensure that the Authentication Devices can communicate with the target DCE server.

2. General Boot-up procedure

The following network information is required for a Xerox Secure Access Authentication Device to communicate with a DCE server:

1. IP Address of the Authentication device
2. IP Address of the DCE server
3. The subnet mask
4. The default Gateway

There are two ways to configure the IP Address of each Authentication Device:

1. Using Static IP values
2. Using DHCP

When configured to use the Static IP address option, any changes made to the settings are stored in the EEPROM however when configured in DHCP mode, the values are NOT stored in the EEPROM. This is important to understand because in DHCP mode under certain conditions the Authentication Device will use values read from the EEPROM.

Xerox Secure Access mode Web Admin Page

It is possible to set the values stored in the EEPROM for both Static and DHCP mode via the Authentication Device web page. In DHCP mode the IP Address, Network Mask and Gateway values will not be stored regardless of which mode is specified -the server address will always be stored.

Configure Xerox Secure Access Authentication Device	
Addressing mode	Static IP
IP Address	192.168.92.88
Network mask	255.255.255.000
Gateway	192.168.092.001
HID decoding	☐

Configure server	
Server IP Address	192.168.092.045

3. Static IP configuration

This is the simplest method for configuring a device. The IP Addresses (see 2. General Boot-up procedure on page 7) are manually entered via the manager mode of the Authentication Devices. Once entered the values are stored in the EEPROM and will be used on subsequent boots of the device. For a description of how the boot procedure executes, see 6. Authentication Device – DCE communication establishment description on page 12.

4. DHCP configuration

Although the Static IP configuration is relatively straightforward to configure, it requires manual configuration of each device; a lengthy task if there are a large number of devices to configure.

The Authentication Devices are able to use DHCP to automatically configure the IP Address, subnet mask and default gateway. Also if configured on the DHCP server, the DCE server address can also be used (see Option 230 below).

DHCP Negotiation fails

If the terminal fails to negotiate with the DHCP server then the IP settings of the Authentication Device are set to:

1. Terminal IP Address = 192.168.2.1 (hard-coded)
2. Terminal mask = 255.255.0.0 (hard-coded)
3. Gateway IP Address as stored in the EEPROM
4. Server IP Address as stored in the EEPROM

If you have multiple Authentication Devices and DHCP fails, all device IP Address are set to the same address (192.168.2.1).

DHCP Negotiation successful

On successful negotiation, the standard IP address values set (IP address, Mask and Gateway) will be used as returned by the DHCP server.

Note: Values returned by the DHCP server are NOT stored in the EEPROM.

Option 230 present

The Administrator can set option 230 on the DHCP server to allow for the configuration of the server field on the Authentication Device.

EQ;A;<DCE Server IP address>

Where the <DCE Server IP address> is the IP address of the server specified in standard 4 octet form, e.g. 192.168.1.23

If the parsing of the string is successful the server IP address will be set to the IP address as specified however if the parsing of the option fails for whatever reason the server IP address is set to 0.0.0.0. A server IP address of 0.0.0.0 will cause the Authentication Device to issue a broadcast bootp request. For details, see 6. Authentication Device – DCE communication establishment description on page 12.

If option 230 is present but is not a Secure Access value, (i.e. used by some other application), the server IP Address is set to 0.0.0.0 which causes a broadcast bootp to be issued.

If there are multiple Authentication Devices and the DHCP server fails to negotiate option 230, the bootp process registers all devices with ALL DCEs alive in the segment. However, only the first DCE that connects to the terminal will work with that terminal.

Option 230 missing

If option 230 is missing then the value of the server address as stored in the EEPROM will be used.

5. On use of the Reset Key

If the Reset key is turned, the Authentication Device will:

1. Set the server IP address to 0.0.0.0 and store the value in the EEPROM.
2. Set the IP Method to use DHCP.
3. Set the password "pc_passwd".
4. Reset the EDI settings to the factory defaults.

6. Authentication Device – DCE communication establishment description

The following describes how the Authentication Device boots.

1. If the Authentication Device has the IP Address of the server, it will send a directed bootp request to the server address; otherwise it will send a bootp broadcast (i.e, if the server IP address is 0.0.0.0, the Authentication Device will issue a broadcast bootp).

   The following information is included in the bootp request.

   - IP Address of the Authentication Device
   - MAC Address of the Authentication Device
   - Terminal Type is set to Xerox Secure Access mode. DCE will ignore any bootp request that does not have the appropriate signature embedded in the request. The signature is Xerox = 'XEFB'
2. Authentication Device waits for a Bootp response. The bootp response must be directed at the Authentication Device.
3. If the Authentication Device does not receive a bootp response in 10 seconds or less, it will sleep for a period of time (up to 3 times, then devices will go to offline mode) and then send the bootp request again (i.e. goes back to step 1.)
   - The sleep times between bootp requests increase based on the sequence of times indicated below until the longest delay is reached (22 seconds) and the time is set back to the last value reached and then the time is reset to the shortest delay (.15s).
   - Sleep times = .15 s, .8s, 2s, 3.2s, 5.6s, 12s, 22s
4. If a bootp response is received by the Authentication Device, the device starts a socket server (TCP) and waits for a client (one client connection only) to connect.
5. If a connection is not made with 4 minutes the Authentication Device will reset and the procedure starts again from step 1.
6. Once a connection is successfully established the Authentication Device waits for a request from the server (DCE) and the boot procedure ends.
7. In offline mode, Xerox Secure Access devices will try to create connection with the server by sending bootp every 30 seconds.

7. Configuration Notes

1. If multiple DCE servers are used then option 230 should not be used when configured for DHCP. Instead, configure the server address via the Authentication Device web page.
2. Using DHCP if one DCE server exists then option 230 can be used to ensure that the server IP address specified is used and changing the address in all of the Authentication Device web pages is unnecessary.
3. Using DHCP is preferred in environments where the server address may change periodically however it is important to ensure that option 230 is used so the server address can be "pushed" to all of the Authentication Devices instead of configuring all of the devices manually.