

Thank you for choosing the Neoteris Instant Virtual Extranet (IVE) appliance! You can install the IVE and start configuring your system in four easy steps:

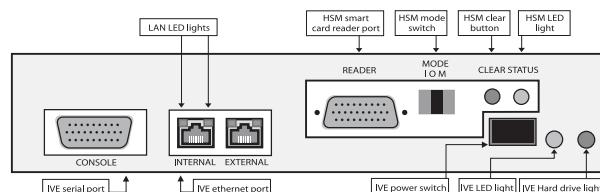
- Step 1: Install the hardware
- Step 2: Enter serial console settings
- Step 3: Perform basic setup
- Step 4: Verify user accessibility

Step 1: Install the hardware

We recommend that you install Access Series FIPS in your LAN to ensure that it can communicate with the appropriate resources, including:

- Authentication servers
- DNS servers
- Internal Web servers via HTTP/HTTPS
- External Web sites via HTTP/HTTPS (optional)
- Windows file servers (optional)
- NFS file servers (optional)

If you decide to install the Neoteris IVE FIPS appliance in your DMZ, make sure that the IVE can connect to these resources.



Access Series FIPS ships with brackets attached to the front of the chassis that you can use to rack mount the Instant Virtual Extranet (IVE) machine. The machine also comes equipped with a built-in hardware security module (HSM) to which you must attach your smart card reader. To assemble your Access Series FIPS hardware:

1. Mount the IVE in your server rack.
2. On the rear panel, plug the power cord into the AC Receptacle and press the power switch to turn on the unit.
3. On the front panel:
 1. Push the toggle switch in the right corner one time. The green IVE LED to the right of the power switch turns on. (The IVE hard drive light (HDD) turns on whenever data is read from or written to the IVE hard drive.)
 2. Plug an ethernet cable into the left port.*
 3. Plug a serial cable from a console terminal or laptop into the serial port.

*The left port uses two LEDs to indicate the LAN connection status

LAN Status	LED 1	LED 2
10 Mbps connection Access 1000/3000/5000	Off	N/A
100 Mbps connection Access 1000/3000/5000	Green	N/A
1000 Mbps connection Access 5000	Orange	N/A
Data is being transferred	Orange, Green, or off	Blinking
No connection	Off	Off

4. On the hardware security module's panel:
 1. Set the mode switch to I (initialization mode)*.
 2. Plug the smart card reader cable into the reader port
 3. Insert one of the smart cards into the reader with the contacts facing up. The green HSM LED turns on. Do not remove the card while the module is in I mode.

*The hardware security module status light indicates the hardware security module's mode:

Module Status	LED 1	Description
Pre-Initialization state	Single, short flashes	The module is ready for initialization
Operational state	Mainly on, but regularly blinks off	The mode switch is set to O(operational). Set to I to start Initialization
Pre-maintenance state	Single, long flashes	The mode switch is set to M(maintenance). Set to I to start initialization

1. Configure the console terminal or a terminal emulation utility running on a computer, such as HyperTerminal, to use these serial connection parameters:
 - 9600 bits per second
 - 8-bit No Parity (8N1)
 - 1 Stop Bit
 - No flow control
2. Press **Enter** until you are prompted by the initialization script.
3. Enter **y** to accept the license terms.
4. Enter the machine information for which you are prompted, including the:
 - IP address
 - Network mask
 - Default gateway address
 - Network interface card (NIC) speed
 - Primary DNS server address
 - Secondary DNS server address (optional)
 - Default DNS domain name (example: acmegizmo.com)
 - WINS server name or address (optional)
 - Administrator username
 - Administrator password
5. Enter the hardware security module initialization information for which you are prompted:
 - Number of administrator cards (We strongly suggest that you create at least two administrator cards and store one in a safe location.)
 - Administrator card pass phrase (Note that you do not need to use the same phrase specified in step 4.)
6. Enter the self-signed certificate information for which you are prompted:
 - Common machine name (example:connect.acmegizmo.com)
 - Organization name (example:Acme Gizmo, Inc.)

The serial console setup is complete after entering this information. When prompted with the option to modify your settings, choose the appropriate option or continue.

Step 3: Perform basic setup

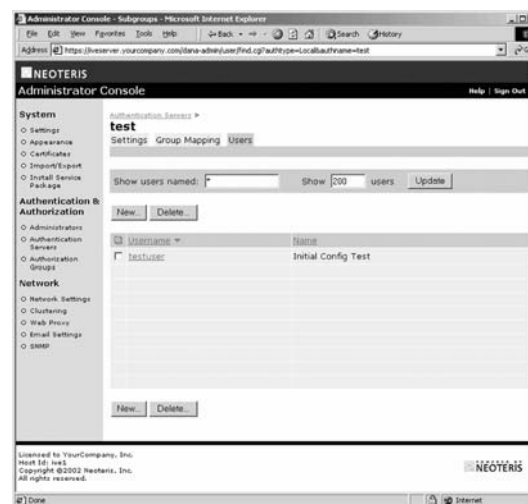
1. In a browser, enter the machine's URL followed by **"/admin"** to access the administrator sign-in page. The URL is in the format: **https://a.b.c.d/admin**, where a.b.c.d is the machine IP address you entered in Step 2-4. If the sign-in page appears, you have successfully connected Access Series FIPS to the network.



Neoteris Access Series FIPS sign-in page for administrators
You must add **"/admin"** to the IVE URL in order to access the administrator sign-in page.

2. On the administrator sign-in page, enter the administrator username and password you entered in Step 2-4 (it's case-sensitive), and then click **Sign In**. The Administrator Console appears.
3. From the main menu, choose **System > Settings > Time**. The **Time** page appears.
4. Specify the machine time and click **Save Changes**.

5. From the main menu, choose **System > Settings > License**. The **License** page appears.
6. Enter your company name and license code in the appropriate fields and then click **Enter**. Your license code information appears on the **License** page.
7. From the main menu, choose **Authentication & Authorization > Authentication Servers**. The **Servers** page appears.
8. From the drop-down list, select **IVE Local Authentication** and then click **Create**. The **New IVE Local Authentication Server** page appears.
9. In the **Name** field, enter **test** and then click **Save Changes**. The **Group Mapping**, **Local Users**, and **User Admins** tabs appear.
10. Select the **Local Users** tab and then click **New**. The **New Local User** page appears.
11. Create a test user by entering a username and a password for local authentication, and then click **Create User**. The test user is added to the IVE local authentication database called "test."



Local authentication server instance with 1 local user record

Step 4: Verify user accessibility

1. To verify that users can access the Neoteris machine, go to a desktop workstation and enter the Neoteris machine's URL in a browser. The machine URL is **https://a.b.c.d**, where a.b.c.d is the machine IP address you entered in Step 2-4. When prompted with the security alert to proceed without a signed certificate, click **Yes**. The Neoteris Access Series FIPS user sign-in screen appears.



User sign-in page

2. Enter the username and password you created for the test user in Step 3-11 and then click **Sign In**. The IVE home page appears.
3. Under **Browse Web**, enter a URL and click **Browse**. The Neoteris IVE browses to the Web site and displays the browsing toolbar on the specified page. Use this toolbar to return to the IVE home page by clicking on the Neoteris icon in the center.

4. Test a few more internal and external sites.
5. In the main menu, click **Windows Files**.
6. Browse to a share and try to download and upload a file. For more information, click the **Help** link at the top of the IVE home page.

After verifying user accessibility, your Neoteris IVE is operational!

Next Steps

To configure and deploy your Access Series FIPS system, perform these next steps:

- Obtain the latest Access Series FIPS OS service package and documentation
- Configure your firewall to enable remote access
- Create a certificate signing request to send to a CA

Obtain the latest IVE service package and documentation

Before configuring your Access Series FIPS machine, we recommend that you log in to the Neoteris Support site, support.neoteris.com, to download the latest build of Access Series FIPS OS and the corresponding Administration Guide PDF and release notes.

Administration Guide provides feature overviews and procedural information for setting up authentication servers, authorizations groups, and access control lists, as well as information for specifying system and network settings.

Configure your firewall to enable remote access

When you are ready to make Access Series FIPS available from external locations, you need to map an external IP address to the Access Series FIPS IP address and open certain ports on your firewall. Specifically:

- Set up your firewall to have an external IP address (sometimes called a Virtual IP) for Access Series FIPS, such as 128.x.y.z. Configure this IP address so that the firewall routes any requests received on port 443 (SSL) and port 80 (HTTP) for the external IP address to the internal Access Series FIPS IP address over NAT (network address translation).
- Set your external DNS to have an external hostname for Access Series FIPS, such as **fiptestserver.yourcompany.com**.
- When deploying Access Series FIPS with the optional DMZ feature, you may alternatively deploy the appliance in dual-port mode to listen for incoming Web and mail proxy SSL connections on an external port. (Refer to the *Administration Guide* PDF for more information.)

When you complete these steps, users simply enter **fiptestserver.yourcompany.com** in any browser from anywhere on the Internet. DNS resolves to the external IP address and tries to connect to port 80. Access Series FIPS accepts the request and immediately sends out a "redirect" to port 443. The browser then requests the redirected URL and users see the Access Series FIPS sign-in page over SSL. After successfully signing in to Access Series FIPS, users have access to enabled resources such as Web, file, email, application, and Secure Meeting servers.

Note: Port 80 is used only to redirect traffic to SSL; no real traffic goes over HTTP.

Create a certificate signing request to send to a CA

Before you deploy Access Series FIPS for enterprise users:

- Create a certificate signing request (CSR) to send to a certificate authority (CA). When the CA returns the signed file, import it in to the Access Series FIPS system. Refer to the *Administration Guide* PDF for more information about importing a trusted server certificate.
- Note that by default, users are granted full Web and Windows network access. To change these settings, configure the Web and Windows access control lists (ACLs) through the Administrator Console.

