iStatus Desktop™

Reducing Frustration for Work-From-Home Employees

In the past few years, the number of Work-From-Home (WFH) users has expanded rapidly. Different companies have different network connectivity for WFH users, with some companies deploying hardware-based firewalls and others using just a PC with a VPN client.

As employees have moved offsite, the role of the IT team has had to adapt. IT teams now need to support the remote user, as well as their home Internet connection that becomes essential to successfully working from home.

iStatus Desktop is an application that can be installed on Windows PCs to perform continuous network testing. The primary goal of iStatus Desktop is to help the end-user understand the problem when essential things are unreachable. In the case of WFH users, iStatus Desktop can be quickly configured by the IT team to monitor the state of the VPN connection and critical servers that the employee needs.

With iStatus Desktop WFH Employees:

- Know if their PC is connected to the Internet
- Know if their VPN to a corporate office is up or down
- Know if other servers they need to access are up or down

Operation

iStatus Desktop is installed in Windows and lives in the system tray (near the clock). It looks just like any other app, and importantly, it never alerts the user about anything that isn't necessary. So on a day-to-day basis, iStatus Desktop quietly monitors things that need to be monitored but never gets in the way. iStatus Desktop doesn't consume a great deal of system or network resources either.

Normally, iStatus Desktop is configured to monitor important resources needed for the employee's job. When a required resource goes offline, iStatus Desktop displays a message to the user, telling them that something they need is not available. Importantly, the messages displayed by iStatus are automatically taken-down (removed from the screen) when problems are resolved. It's also easy for the end-user to pause alerts for any target, so they can continue working.
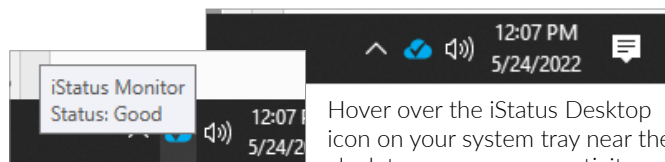
Hover over the iStatus Desktop icon on your system tray near the clock to see your connectivity status or click for more details.
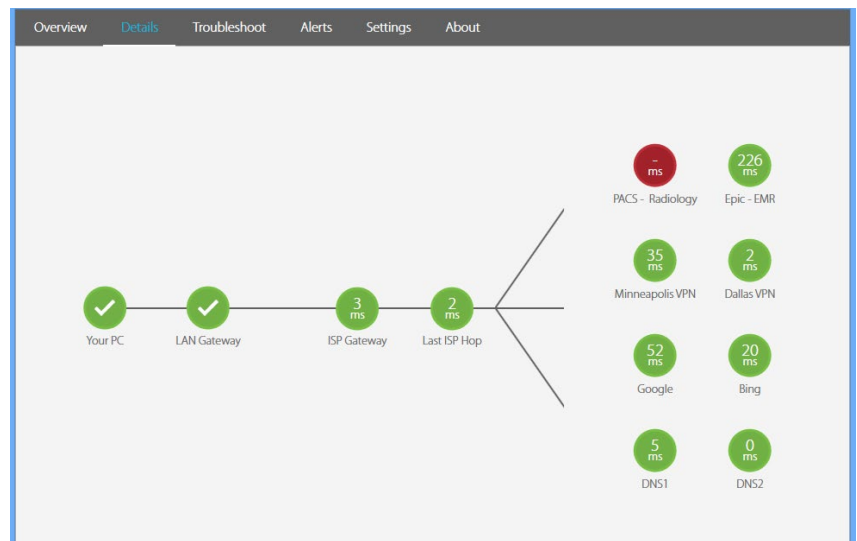
Advanced Features

iStatus Desktop can also work in conjunction with Akative RocketFailover® and will inform the user when the failover connection is active. iStatus Desktop has several other features that make it a good choice for WFH deployments:

- Configuration can be protected with a pin-code.
- Hosts can be monitored with ICMP (ping), HTTP, or HTTPS.
- iStatus ArpWatch™ security can be enabled or disabled to monitor for network security events.
- Alerts can be set to; hidden, small or large
- Configuration export and import features allow configurations to be saved and used across multiple users.
- Monitored hosts can be set to generate or not-generate alert messages. This allows iStatus Desktop to potentially never interrupt the end user if desired.
- iStatus Desktop supports 33 different languages.
- It can be integrated with Akative RocketFailover to inform the user when a failover (secondary) Internet connection is activated.
- It can be configured to log events so that the IT team can view them to diagnose issues.

Effortlessly gain visibility, eliminate guesswork, and increase network security with iStatus Desktop!
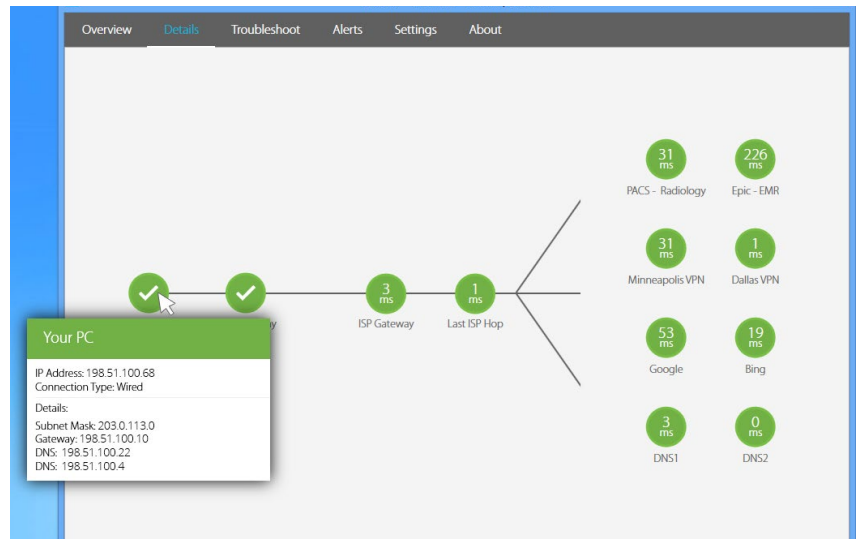
Quickly get information about the connection.

Easily identify where issues are occurring.

Learn more about issues occuring on the Alerts screen.
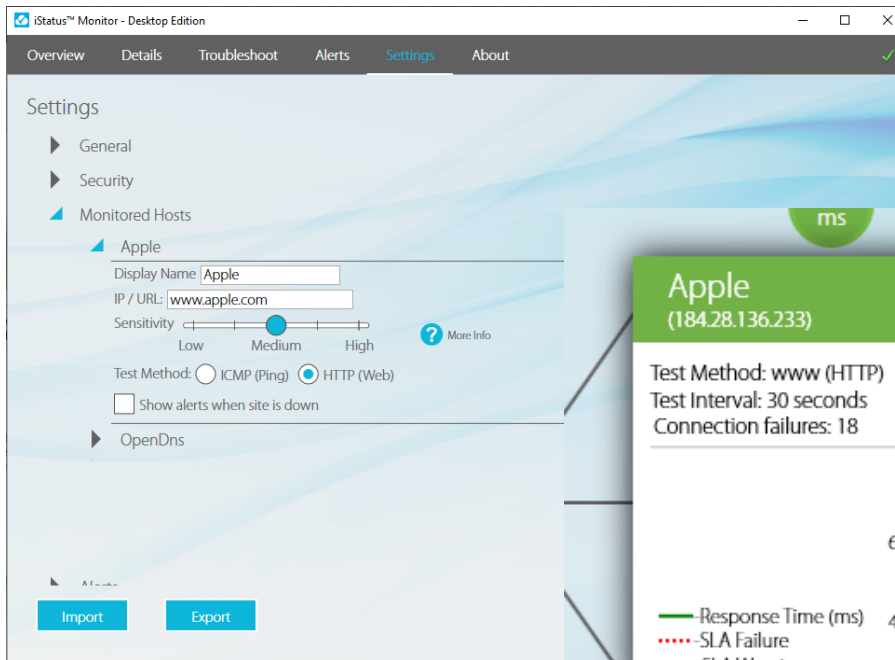
Effortlessly setup hosts to monitor and the desired sensitivity for each host in the Settings screen.

Hover over the host in the Details screen to view the historical information of the host, such as the performance, total downtime, and response time.

iStatus Desktop is a Valuable Tool for IT Teams

If you've ever endured the pain of talking a non-technical user through the process of finding their IP address, figuring out if they are on a wired or wireless network, or if their PC is getting DHCP, you will appreciate the value that iStatus Desktop provides.

When users have connectivity issues, having iStatus Desktop installed on a WFH computer allows the IT technician to more quickly diagnose the problem. IT teams can quickly gain the following information:

- Are the hosts up/down
- Is the Internet connection up/down
- What is the IP address of the PC, network mask, and DNS servers being used
- What is the IP address of the LAN gateway, and can the PC see the gateway
- Is the PC using a wired or wireless network connection
- Is the ISP gateway up/down
- Is the user able to access other websites or key resources on the Internet
- What did the Internet path look like when it was last working

- Is this problem a one-off issue, or is this happening frequently
- When sites are offline, how long are they down
- Under the direction of the IT team, WFH users can easily right-click a monitored target to open a ping against the target (bypassing the need to talk users through the process of opening a command prompt and typing commands)
  - Quickly right click and ping the LAN gateway
  - Quickly right click and ping any monitored host