PROXY Pro v10 RAS – Security Layer Overview

Proxy Networks remains on the forefront of the remote desktop and remote support software industries by keeping security and data flow concerns as paramount. This document describes each layer of security in detail. We're committed to providing a secure, scalable, reliable remote desktop platform for the modern business with multiple layers of security in order to meet a wide variety of use cases and requirements.

1. Authentication

For PROXY Pro v10 we delegate authentication to a new component called the PROXY Identity Manager which implements multiple identity providers like Windows Authentication and Azure Authentication. This new architecture lays the groundwork for the inclusion of additional identity providers moving forward. New for v10, the software also supports hierarchical grouping and Active Directory synchronization so that Hosts are organized into groups that match how they're organized in Organizational Units within Active Directory.   Prior to PROXY Pro version 10, we were tied to Windows Authentication via SSPI. In v10, we broke that tight integration and developed a separate identity manager. This allows for much more flexibility to use alternative authentication protocols and support 2-factor authentication schemes. Once a user authenticates when starting Proxy, they are not asked to authenticate again when connecting through to a remote machine.

In the event that an employee were to leave your company, but has been given user rights within Proxy, simply disabling the account in Active Directory (or changing the password) will lock this user account out of Proxy entirely.

The PROXY Pro v10 RAS (formerly branded as the Private Cloud Edition) uses a hub-and-spoke connectivity model. The PROXY Pro Hosts and PROXY Pro Masters are the spokes, clients and viewers respectively, that communicate with your server. While the product is designed to have all connections routed through the server for accurate centralized auditing, it's entirely supported and possible to connect in a Peer-to-Peer fashion via the PROXY Pro Master's "Peer-to-Peer Hosts" tab.

The Host has its own set of security settings found on the Proxy Host Control Panel's Security tab > Set Permissions. You'll see **Data Services Security, Admin Security and Settings Security tabs** where local administrators have full control and administration in all areas by default while non-administrators would not. Security settings are controlled by Windows user accounts and groups and are highlighted below.

Data Services Security – Who can connect and what rights they have (i.e. File Transfer)
Admin Services Security – Who can open the Host Control Panel, terminate session
Settings Security – Who can view and edit Host Control Panel settings

2. Authorization

Aside from granting users the ability to access remote machines, Proxy allows you to define, at a very granular level, what specific pieces of Proxy functionality will be available when users make connections. For example, you may decide that not every Proxy user should have the ability to perform file transfers, perform remote administration tasks or initiate screen recordings. This is ideal for multi-tiered helpdesks if separate teams are responsible for supporting specific sets of machines. The same logic also applies when you would like to temporarily grant an outside contractor access to one or more computers.

Each customer’s PROXY Pro Web Console’s ”Accounts” tab would be populated with the users and groups that shall have access to one or more groups of machines. **Administrative** users have full control of their web console instance, including controlling user access, generating connection reports and changing settings. Users designated as **Master** users may be granted access to one or more groups of Hosts but will not be able to perform administrative tasks. The third account type, **Personal** accounts, allows a user to log in and connect to one and only one machine, typically their work computer, ideal for use by VIP members of your organization. Personal accounts securely extend remote desktop access to work-at-home employees.

Administrative Account Users

- Full control and administration of a Proxy Web Console
- Access to all 7 web console tabs, including Accounts, Activity, Analytics, Gateway
- Typically held by an IT Director, Support Manager, Network Administrator

Master Account Users

- Access to one, many or all groups of Hosts as defined by an Administrative user
- Access to 3 tabs including available Hosts and Recordings tab
- Typically held by helpdesk users, folks in IT (non-admins of the web console)

Personal Account Users

- Access to a single computer as defined by an Administrative user
- Designed for use by remote users and work-from-home staff
- Typically held by VIP members or remote users at an organization

New for PROXY Pro v10, defining access and authorization policies have been enhanced in that hierarchical Host grouping structures have been added to the product. For example, if you have Support Teams in multiple physical locations, responsible only for their region, it’s now possible to create sub-groups (like AD containers) and set security on them. Each of your Host machines can be sent to their appropriate groups in your web console by way of the software’s Automatic Host Grouping feature enabled by an administrative user. As Hosts get deployed to computers within your organization, your groups will begin to populate and they will become available for connectivity to authorized users.

3. Encryption

By default, all connections made with Proxy Networks software use AES encryption (256-bit key) with the SHA1 hash. The other optional (non-default) choices for encryption algorithms include Triple-DES encryption (192-bit key) and also RC4 encryption (128-bit key), both with SHA1 hash. Furthermore, the screen capture technology is Proxy's very own, and has been completely proprietary since its development in 1993.

4. IP Address Restrictions

Available with the TCP and SSL protocol (not UDP), the Proxy Web Console can be configured to only allow incoming connection attempts that originate from a definable IP address range(s). Consider creating an "Allow All Except..." or a "Deny All Except..." list to help mitigate any potential brute force attacks from malicious parties.

Best practices may include whitelisting your internal range from the IT side, so that your server completely ignores inbound connection attempts from all other source ranged. We understand that your router and/or firewall software will be the bigger tool for the job. For those without, this feature should serve its intended purpose for you well.

5. Ports and Protocols

Although all connections are fully encrypted over UDP and TCP, we also support the ability for connections to use SSL. If you require that all available security avenues be pursued, this can further help you ensure that your data is kept secure. New for PROXY Pro v10, we also now support Web Sockets and Secure Web Sockets and now enforce TLS 1.2. Please see below for port usage requirements.

PROXY Pro RAS: Inbound 2303 TCP, 2303 UDP, 443 (SSL), 8443 TCP (SSL)
PROXY Pro Host: Inbound 1505 TCP, 1505 UDP

6. Options for End-User Permission to Connect

The PROXY Pro Host is set by default to allow remote connections with no user permission required. That said, the software can be very easily configured to either require end-users to grant permission, or to accept or deny after a specified time. The three permission behaviors settings are:

- **No Permission Required** - Connections will be made without end-user intervention (the default)

- **Permission must be granted** - Connections will only be made after an end-user explicitly allows the connection, and the connection will be rejected if the user does not allow it within the specified timeframe (10, 30, 60 or 120 seconds).

- **Permission request from Host; connect if no response -** This option gives the end user the courtesy of allowing the connection, but will allow you to connect to the machine if there is no response from the end user within the specified timeframe. Additionally, if there's no response, you can choose to allow the connection, but lock the workstation so that you're required to actually log into Windows to begin using the machine.

**Note that although machines may be configured to require end-user consent for connections to occur with Proxy, there is also a "Permission to Connect Over-ride" which can be applied to specific user account(s) if desired. This special over-ride is designed to accommodate situations where an emergency access process is required.*

7. Real-Time Reporting

Available to an administrative user, the PROXY Pro Web Console's Activity tab reports the identity of each person that is currently logged into the Proxy Web Console or is using an installed PROXY Master, along with which machine(s) they're connected to presently. Additionally, Hosts with in-progress screen recordings are listed as well to provide you with any and all remote desktop activity.

- **Account Activity** – Uses presently authenticated to the server
- **Host Activity** – Host machines with a connection in progress
- **Recording Activity** – Host machines with a screen recording in progress
- **Reverse Connections** – Host machines reporting in externally to the LAN

8. Auditing & Analytics

Available to an administrative user, the PROXY Pro Web Console's Analytics tab reports on all connections that have occurred in the past. Specify a username and get a complete history of all connections made by that user. Conversely, you may specify a particular machine and have Proxy provide you with a listing of all connections made to it, and by whom (and when) those connections were made. Results are ready to be printed or exported to .CSV or .XLS directly from the blue navigation bar. The Proxy Web Console's "Analytics" tab breaks audits down into the following four tabbed sub-categories:

- **Connections Audit** – Generate report of logins and logouts by time and by who
- **Services Audit** – Generate report of connections made to Hosts by time and by who
- **Recordings Audit** – Generate report on recordings by Host or by user
- **Licenses Audit** – Generate a report on license usage over time

9. Clientless Support

The "Share my Desktop" button on a PROXY Pro Web Console's landing page allows an end-user to activate a temporary instance of the Host, named the "Host on Demand" which then allows authorized web console users to connect and provide attended end-user support on a true on-the-fly basis. The Host on Demand instances automatically report to a group keenly called "Host on Demand". The beauty of the Host on Demand is that there's no software installation that occurs, it can be run by a non-administrative user, and can be deactivated and removed from any given system by the user at any point. Once removed, you will no longer see them on your list of available Hosts from your Proxy Web Console.

Technology-wise, Proxy Networks has selected Microsoft's "ClickOnce" as the means to deliver an installation-free Proxy Host that allows the machine to be remotely accessed from your Proxy Web Console. Unlike the traditional (installed) Proxy Host which runs as a service and is therefore always on, the Host on Demand instead runs as a process only during the user's current Windows session.

Pinning the Host on Demand can be accomplished by right-clicking the panel and choosing the third option. This will cause the Host on Demand to stop running as a process and to re-launch as a service, therefore functioning the same as the installed Host except that the end user can stop and remove the Host on Demand from the system at any time. The key benefit is that the Host on Demand allows for remote support sessions to be possible without leaving a remote desktop client on the machine after the session has ended.

For general information about Microsoft's ClickOnce technology, we recommend this particular resource from Microsoft's knowledgebase: http://msdn.microsoft.com/en-us/library/142dbbz4(v=VS.90).aspx
For ClickOnce Cache information: http://msdn.microsoft.com/en-us/library/267k390a(v=vs.90).aspx
And to clear ClickOnce Cache: http://blogs.msdn.com/b/karstenj/archive/2006/08/09/693488.aspx

Please contact us with any questions at 1-877-PROXY-US
or email support@proxynetworks.com