PROXY Networks

Feature Comparison Matrix

Microsoft System Center Configuration Manager

Key Features	Description	Microsoft SCCM Remote Control	PROXY Pro Private Cloud Edition
(1) Internal Connectivity	Connect to machines within your LAN	Yes	Yes
(2) External Connectivity	Connect to machines outside of your LAN	No	Yes
(3) File Transfer	Transfer individual files or entire directories	No	Yes
(4) Chat	Open a chat window between the you and the end user	No	Yes
(5) Screen Recording	Record screen activity on a remote machine with or without being connected for remote control	No	Yes
(6) Screen Recording Playback	Play screen recordings from any machine & convert to .WMV	No	Yes
(7a) Listing of Machines	View available machines by computer name	Yes	Yes
(7b) Listing of Machines	View available machines by logged-in username	No	Yes
(7c) Listing of Machines	View available machines by logged-in username as well as the user's computer name	No	Yes
(8) "Stealth Mode"	Connect to machines silently without alerting end users	Yes	Yes
(9) Connect only with end-user consent	Connect to machines only after an end-user has explicitly granted you the ability to connect	No	Yes
(10) Many-to-One Connectivity	Multiple technicians may connect to the same target machine for a true collaborative support session or meeting	Yes	Yes
(11) Active Users List	View a list of all connected users (by Windows account) when two or more technicians are connected	No	Yes
(12) Centrally Define Access	Create access policies from a centralized management console to define which users may connect to machines	Yes	Yes
(13) Defining Granular Access	Define which additional functional abilities are available when technicians connect (File Transfer, Chat, Clipboard)	No	Yes
(14) View, Edit and Manage Computer Settings	Access to the target machine's registry, task manager, service control manager from the connection window	No	Yes

Feature Comparison Matrix

Explanation and Breakdown of Proxy's Capabilities

(1) Internal Connectivity - The Proxy Web Console uses a "hub-and-spoke" connectivity model whereby endpoint machines (the spokes) report into the server running your Proxy Web Console (the hub) using, UDP port 2303 (by default). Note that UDP, TCP or even SSL can be used over any port of your choosing.

(2) External Connectivity - Not only does the Proxy Web Console allow you to connect to endpoint machines within your network, but also to machines that travel outside as well. For internal connectivity, the Proxy Hosts are configured to report into the LAN IP address of the server running your Proxy Web Console. For external connectivity to be possible, simply port forward UDP port 2303 to the LAN IP address of the server, so that your Host machines can report to your Gateway's public IP while your router or NAT device takes care appropriately routing inbound Hosts to your server.

(3) File Transfer - When connected to a Proxy Host machine, you will notice the "File Transfer" tab at the bottom of the connection window. Your local machine's file system and directory structure will be listed in the left-hand pane, and the remote machine's file system is listed on the right. Navigate to the desired locations on each machines' file system and simply "drag and drop" individual files or entire directories from one side to the other. If you are transferring large files and either side of the network connection suffers a disruption, we have a "resume" capability once connectivity is restored.

(4) Chat - If you are unable to use the phone to communicate with users, a technician may connect to the end-user's computer and click the "Chat" button found at the top of the connection window to begin communicating with the user on the Proxy Host computer.

(5) Screen Recording - If you would like to record the support session, you may trigger a screen recording to begin when you've connected to an end user's Proxy Host computer from the Proxy Web Console. However, you can trigger the screen recording to begin without actually connecting to the end user's computer for remote control. When you start the recording, you will be asked how long the recording should be (in minutes). The resulting files will be stored within the installation directory of Proxy on your server, to enter a duration (in minutes)

(6) Screen Recording Playback - Recordings can be played back from within your Proxy Web Console, or from the installed Proxy Master viewer. Note that recordings can be exported from Proxy's proprietary format (.PrxRec) to a format that can be played back in your favorite media player (.WMV). This can be used either for quality assurance, monitoring employees, or even to create a library of training videos that show end users how to perform certain tasks.

(7) Listing of Machines - Configuring how you would like your Proxy Host machines to be listed to you

(7a) By default, Proxy Host computers are presented in your list by their NETBIOS computer name.

(7b) If you'd like your machines to be listed to you by the identity of the person on the Host, you can do so in either of the following formats depending on your use cases. Either have them listed to you in the format of "DOMAIN\jsmith" or simply just "jsmith".

(7c) Should you prefer that your machines be listed with both the identity of the user as well as the name of the computer, the Proxy Hosts can appear to you in the format of "DOMAIN\jsmith on DELL-XPS-123 or "jsmith on DELL-XPS-123"

(8) Connect in "Stealth Mode" - By default, connections made to Proxy Host computers will cause a "Toast" notification to appear to the end user in the bottom-right hand corner of their screen. Also, the Proxy Host Tray Icon changes from yellow (when no connection is in progress) to green once a technician has connected. In addition to these visual notifications, the Proxy Host can emit beeps from the PC speaker when connections are made and closed. Note that each of these can be individually enabled or disabled depending on your use cases and/or remote access requirements.

(9) Connect only with end-user consent - The Proxy Host can be configured such that end users must explicitly click an "Accept" button when a connection is attempted by a technician, otherwise the connection will be refused if the end user does not allow the connection within 10, 30, 60 or 120 seconds. Also, note that there is a second mechanism that still allows the end user the courtesy of being able to click "Accept", the difference with this second option is that the technician will get connected after the time period expires if the end user has not explicitly denied the connection. Furthermore, with this option enabled the Proxy Host can either be configured to "Lock" the workstation so that the technician must log into Windows before actually using the computer, or the technician can be brought directly to the Host machine just as it was left by the end user. Note that there is an over-ride to the "Permission to Connect" feature, which can be applied to certain members of your support team's user accounts.

(10) Many-to-One Connectivity - Multiple technicians may connect to the same Proxy Host computer for a true collaborative support session, or even a meeting.

(11) Active Users List - In the event that multiple technicians are connected to any given Proxy Host computer and it's important that your end users know this, you can enable this window that lists the identity of each connected user, by Windows account, and also the IP address that they are connecting from.

(12) Centrally Define Access - The Proxy Web Console allows an IT director or LAN Manager to centrally define which technicians, by user accounts, are permitted to connect to which Hosts or groups of Hosts.

(13) Defining Granular Access - Not only can you enable or disable the ability for technicians to connect to a Proxy Host computer for remote control, but you this can be taken a step further by allowing/disallowing additional Proxy functionality. Some of the functionality that can enabled or disabled centrally would be the ability to perform file transfers, print remotely, copy/paste clipboard content in and out of the Host machine, initiate chat and even screen recordings - ensuring that remote access is locked down as best as possible especially in dispersed environments.

(14) View, Edit and Manage Computer Settings - When connected to a Proxy Host machine, there will be a "Remote Management" tab at the bottom of the connection window (which can be enabled or disabled for certain technicians) that allows you to view Windows Event Viewer logs, kill running processes, start/stop/restart services from the Service Control Manager, make registry edits, force a log off of the console user, view a listing of hardware and installed software - all of which can be done from this tab, behind the scenes and completely transparent to the end user.

For more information please contact Proxy Networks and ask for a live demo with our Sales and Support Teams.