Xerox® ConnectKey® Technology
Remote Control Panel
White Paper

Table of Contents

The information presented in this document is broken into the following sections:

Section 1 – General Overview

Xerox® ConnectKey® Technology provides an environment for operating and managing Xerox® multifunction printers (MFPs). A Web-enabled Remote Control Panel feature is available on all Xerox® devices built on ConnectKey Technology and may be accessed as a client from any IP connected workstation.

Remote Control Panel enables a user to view and operate the MFP user interface (UI) via a Web UI without being present at the physical device. This capability has a variety of applications and benefits throughout a product's selling cycle and use. It can be used to demonstrate the product to prospective customers, to facilitate customer training and to provide real-time customer support.

Remote Control Panel also significantly enhances the management and servicing of ConnectKey enabled MFPs. The user roles for this feature are defined as General User, System Administrator (SA), and the Authorized Service Representative or Customer Service Engineer (CSE), each having their appropriate levels of access and control.

The Web UI provides a remote emulation of the device control panel in which both the hard and soft buttons are displayed and functionally operable on the client's workstation. All user and administrator functions on the device can be accessed and operated remotely.

Screen shot of the ConnectKey Technology-enabled MFP user interface emulation displayed on a user PC. UI soft buttons and control panel hard buttons are fully operable using a local mouse and keyboard.

The Remote Control Panel feature was designed for ease of use and robust security. Feature setup and user access is accomplished through the "Support Tab" in the device Web UI. This incorporates the function into a currently existing and well known tool, enabling it to be fully integrated in existing device access, authentication and authorization controls.

Section 2 – Enabling the Feature

The Remote Control Panel feature is off by default at the initial device installation and must be enabled by the System Administrator, provided the device has been set up with admin privileges. Enablement, setup, and use are all accessed in the "Remote Control Panel" page of the device Web UI support tab. Selecting this page displays the configuration and access sections. Selecting the configuration's edit button enables the System Administrator to enable the feature and select permissions in a single step. If the Web UI user has not yet been authenticated as the System Administrator, the system will present the appropriate login screen. The remote connection requires a Secure Socket Level (SSL) link to the device, which is automatically enabled for this feature. No additional setup is required.

Section 3 – Authentication, Rights and Permissions

When the Remote Control Panel feature is enabled, the permissions selections must also be set from the three available choices, which are 1) Admin only, 2) Admin and Diagnostics users and 3) All Users. These choices only apply those users who are actually authorized to launch a remote session.

- Admin only – This selection requires a System Administrator to log into the Web UI prior to launching the remote session.
- Admin and Diagnostics Users – This selection requires either a System Administrator or CSE to log into the Web UI prior to launching the remote session. When the CSE is authenticated in the Web UI and a remote session is launched, the remote control panel displayed on the client workstation includes pathways to enter the device diagnostics mode.
- All Users – Any user can launch a remote session without having to authenticate in the Web UI.

While these user roles are consistent with the device roles and privileges, authentication in the remote Web UI and the local MFP device UI remains separate. For example, a System Administrator who logs into the Web UI then also needs to log in to the device as a System Administrator in order to access the admin level content of the device. In this way, the permissions scheme preserves the existing access policies of the device beyond access to the Web UI.

Session timeouts are another example of how the Remote Control Panel maintains existing device behaviors. Here the feature adheres to both the Web UI and device session timers. If a remote user is logged into the device and the device session timer times out (e.g., due to inactivity), the user is automatically logged out but the remote session stays connected with the device in the non-authenticated state. To prevent leaving the device in an authorized state, any authenticated user at the device is logged out when the remote session is terminated for any reason. To prevent leaving an unattended session connected indefinitely, the remote session is terminated when the device enters power saver or if the Web UI times out.

User Collisions

Xerox® ConnectKey® Technology is set up to allow only one remote user connection at a time in order to prevent confusing situations or security/privacy issues with multiple users. If a need to share the session with multiple users should arise, sharing can be done via the client workstation through any of the widely available native or third-party desktop sharing tools.

If a remote session is attempted when a session is already active, a busy message is displayed in the Web UI. However, an Admin Priority feature is available. If the System Administrator is logged into the Web UI and attempts to launch a remote session when one is already connected, the busy message will provide an option to disconnect the previous session.

The concept of a busy MFP also applies when a remote session is connecting to a device currently in use. Remote Control Panel first checks to see if the local device is busy and if so, asks permission to connect a remote session. The system checks the local UI (LUI) session timer as an indication that a local user is operating the device control panel. If there is an active local session, a pop-up message on the LUI asks the user to accept or deny the remote session. If denied, the session does not connect and an associated message is displayed on the remote Web UI. If the local user accepts, the session is initiated. If the request for remote connection times out (e.g., the user walks away from the device without responding), the session does not connect and an associated message is displayed on the Web UI.

The Admin Priority feature also applies if the accept/deny message times out and provides a way to override the session if the remote user is authenticated in the Web UI as the System Administrator. The Web UI message offers a selection option for overriding the existing local session by terminating it and then launching a new remote session.

When a remote session is initiated to a device with no active LUI session, the connection is made without the need to accept or deny the request.

Section 4 – The Remote Session

The Remote Control Panel leverages Virtual Network Computing (VNC) technology, employing a VNC server and a VNC viewer that are fully integrated into the device software. The VNC server is integrated into the MFP's graphical user interface server that drives the LUI and user input devices such as keyboards, mouse, etc. The VNC viewer is temporarily served to the client's browser in a Java applet form. The applet runs and connects to the machine's VNC server port and is removed from the client workstation when the session is terminated. The feature will only work with the applet supplied by Xerox. Customers are thus not required to install third-party applications or software on their workstations, avoiding needless complications.

When a remote session is requested, a SSL encrypted secure session is first established by setting up a secure tunnel from the device to the client. This method of connection opens a variable network port for the duration of the session. The port assignments are randomized and closed when the session is terminated. This avoids a situation in which a static open port is always available on the device. If for some reason the sockets are created and the connection is set up, the applet won't connect. Instead, the system will reset, clear the connection and close ports. During this time the system will not accept any Remote Control Panel requests for 60 seconds.

Screen shot showing Remote Control Panel tab and "Open Remote Control Panel" button in the Web UI.

Launching a Remote Session

The user requests a remote session by navigating to the Web UI "Support Tab/Remote Control Panel" page. Selecting the "Open Remote Control Panel" button initiates a connection with the device and displays the hard/soft panel emulation in a separate popup frame. This enables multiple devices to be viewed simultaneously on the client workstation (browser dependent). When the connection is initiated, it automatically wakes the device from power saver mode (if asleep), the secure tunnel is created and the Java applet is served.

Once the session is fully connected, both the local and remote users have control of the hard and soft buttons. This is referred to as "Dual Control Mode" and is particularly useful when a local user and remote user are collaborating, such as when a remote help desk is assisting or training a user at the device.

A number of advanced Admin or service functions are better served if there is no interaction from a local user. A setting is available on the Remote Control Panel page to block the local control panel. In this mode, a remote user can initiate a remote session in which the local control panel keys are locked out. This ensures that settings can be entered remotely without local user interference. If a local user attempts to use the control panel while in this mode, a warning message is displayed on the device UI for a few seconds. This mode is cleared when the session is terminated, at which time local control panel operation is restored.

Browser Support

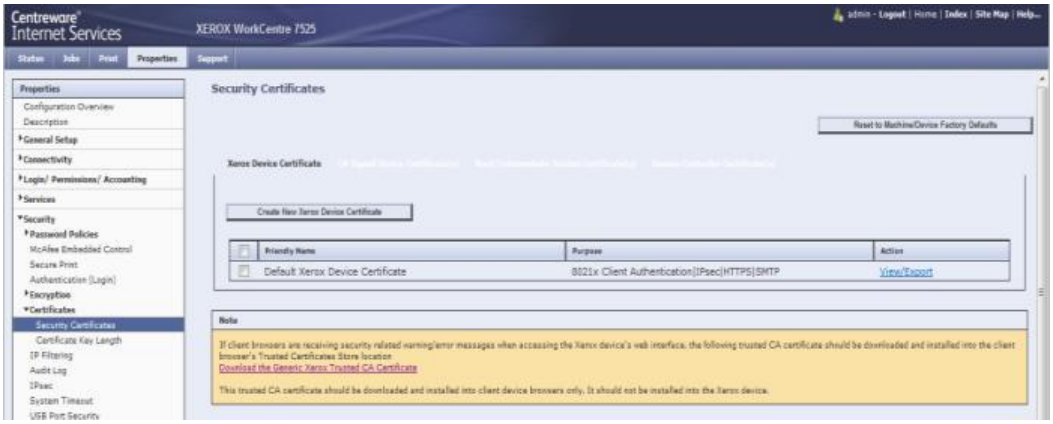
Remote Control Panel functions with any browser that supports the device Web UI. However, various browsers have differences in behavior, which could cause slight differences in the Remote Control Panel presentation. For example, the ability to view multiple devices simultaneously on the client workstation is browser dependent. As of this writing, multiple viewing functions as described with Google Chrome™ and Mozilla® browsers but not Microsoft® Internet Explorer® 8/9. Internet Explorer 8/9 utilizes only one pop-up window and displays only the most recent Remote Control Panel session.

Browser Magnification

The setting for Remote Control Panel viewing is determined by the browser's zoom setting. While the zoom setting defines the browser window in which the Remote Control Panel is displayed, it does not change the scaling of the UI's graphics. The emulation is optimized for a zoom magnification of 100 percent within a browser window. If the browser zoom is set to less than 100 percent, the window will be too small and some portion of the Remote Control Panel will be truncated. If this occurs, the user can correct the situation by closing the session, resetting the browser zoom to 100 percent and relaunching Remote Control Panel.

Browser Certificates

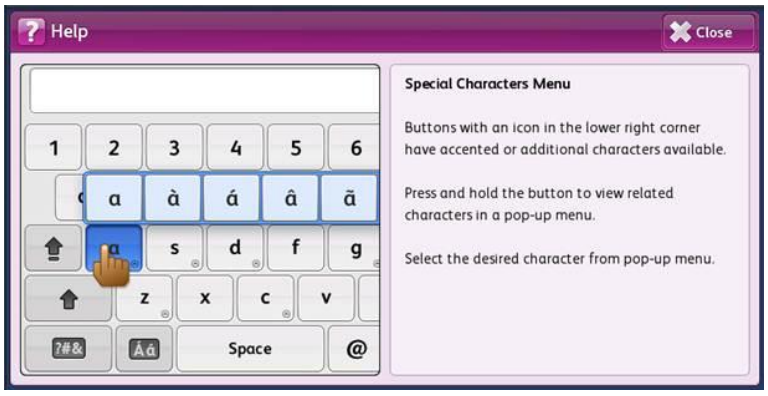
When the browser attempts to connect to the device, it will check to verify the authenticity of the device by checking the security certificate. If a mismatch is observed, the browser will display a message warning the user that the connection cannot be verified or that it is untrusted. The user can generally accept the warning and move on, but this will reoccur each time a session is launched. The device Web UI provides a mechanism to download the Default Xerox Device Certificate to mitigate this situation.



Screen shot showing option to download the Default Xerox Device Certificate.

Special Characters Menu

The Remote Control Panel emulates the same behavior as the local control panel when the user inserts special characters. The following illustration shows how to insert an accented letter “a” on the device local panel. To select this character on the remote panel, the user will click the mouse on the character “a” and hold it until the pop-over is displayed. Release the mouse button and then move pointer and click on the desired sub-key.



Screen shot showing UI instructions on how to insert a special character.

Section 5 – Security

The Remote Control Panel was designed with security as a primary objective. The following list describes some of its security features and attributes.

- Xerox® MFP devices are shipped with the Remote Control Panel feature disabled. It requires a person logged in with System Administrator PIN or credentials to activate the feature and set up the permissions.
- The System Administrator has the ability to disable the Remote Control Panel in the Web UI at any time. Only the System Administrator can enable/disable the feature. Neither action requires a reboot of the machine or client workstation
- The System Administrator has the ability to restrict which users can use this feature. (SA only, SA and Diagnostic Users only, all Users)
- Remote Control Panel adheres with the device's existing authentication and access models, user permissions, accounting, and does not circumvent device permissions.
- An accept/deny message is displayed to the local user when a remote session is being connected to a device currently being used. If the request for remote connection times out (e.g., the user walks away from the device), the message displayed on the Web UI allows the System Administrator to override the session.
- Only the System Administrator is allowed to terminate another user's remote session
- Remote Control Panel utilizes the device SSL mode when a session is initiated. Even if SSL is disabled in the Web UI communications, SSL will be automatically used for Remote Control Panel sessions. The Remote Control Panel uses FIPS-compliant cryptographic algorithms.
- Communication ports between the client workstation and the device are automatically created when the session is initiated and closed when it is terminated. A random port assignment is used and only one session is allowed at a time.
- The soft keyboard normally highlights the keys to enhance ease of use. These key presses are hidden when inputting text in any masked field, e.g., "Password." This prevents remote users from determining passwords when entered at the local UI.
- Remote Control Panel supports the Java applet security model, which has been designed to protect the user from malicious applets. The Remote Control Panel client (served as an applet) can only communicate with the machine that sent it and only on the port (randomized) it is assigned to. In addition, communication is encrypted and the applet itself is obfuscated and is not readable. Because the applet temporarily places the Remote Control Panel client on the user's workstation, its use eliminate the need for users to load permanent software on their systems. When the session is terminated, the applet and Remote Control Panel client are removed.
- Xerox® ConnectKey® Technology is a closed, embedded environment and not an open Java platform, as might be found in a PC environment. Using the Remote Control Panel applet should not be confused with the device's capability to support user-initiated Java applications.
- The device audit log records Remote Control Panel activities, logging session initiation and termination, and when the feature has been enabled, disabled or configured.

Several indications alert local users to an active remote session status at the device. When a remote session is being initiated, a full screen message is displayed on the LUI. This message must to be satisfied with an "Accept "or "Deny" response if the device is in use. Once the session has been connected, a status message is displayed in the SR2 region and a remote user role is displayed in the LUI soft Login/out button.

Section 6 – Device Service and Safety

The Remote Control Panel does not impact the device safety in any way when used in normal customer mode, but special considerations are included to support Remote Service Diagnostics.

General User and SA Related Functions

This category includes all users operating the device in normal customer mode such as general MFD user, System Administrator, help desk support, IT support, training, etc. This feature allows the device control panel (both hard and soft buttons) to be operated remotely, but does not offer any additional capability beyond the default controls accessed locally from the device or remotely through the Web UI. This feature does not circumvent any of the safety features of the machine. For example, many Xerox® MFPs are designed for remote access, such as Web UI, Xerox® CentreWare® Web, etc., and remote operation through printing, remote job submission, faxing, etc. The devices are safeguarded from local user hazards as they start and stop on their own and are designed for unattended operation.

Service Related Functions

Servicing the device requires additional safety consideration because service personnel access special non-customer modes and can potentially circumvent the safety features. For example, trained service personal have the skills and training to run diagnostic procedures with covers and access panels removed from the machine. This feature was designed to enhance the service function by maintaining the service safety considerations while enabling remote service access.

The remote service initiative for Xerox® Office products is working to eliminate CSE visits to machines and reduce the number of broken calls. The concept is to put a program in place with the customers to triage the machine remotely when a customer calls for service. The goal is to fix the machine without a service visit or obtain critical information to prevent a broken call if a visit is warranted. The list on the following page includes descriptions of the relevant features and controls that are implemented in this mode.

Screen shot showing Service Info tab open on Remote Diagnostics page.

- Access / Permission – The Diagnostic User role (CSE) available in the device was extended to the Web UI, enabling diagnostic users to login with their respective credentials. To access service functions, the System Administrator has to set the feature access permissions for Diagnostic User access. Once set, the CSE needs to log into the Web UI with Diagnostic User name and password and initiate the remote session. The remote control panel displayed for the CSE has an additional "Diagnostic" button displayed.

  This provides access to existing device diagnostic login and pathway screens. The respective device service mode passwords can be entered in the appropriate screens remotely.

- Remote Session – Since only one remote connection at a time is allowed, a CSE can be viewing the device remotely without concern that another non-CSE session can also connect. In addition, the CSE can block the local UI when initiating a session to protect the machine during remote service procedures. When the device is in this mode, the local user is notified by a message that the local panel hard and soft keys are not functional at this time.

- CSE Only Access – If the device is in service mode (local CSE at the device) when a remote session is initiated, the session will only connect if a CSE is authenticated in the Web UI. This will prevent non-CSE users from connecting into the device while it is being serviced locally.

Remote Service Safety

When service personnel connect to the device remotely to provide some service actions, they cannot expose the machine to physical interactions such as opening covers or cheating interlocks. They can only access whatever can be displayed on the UI, which cannot harm a person at the device.

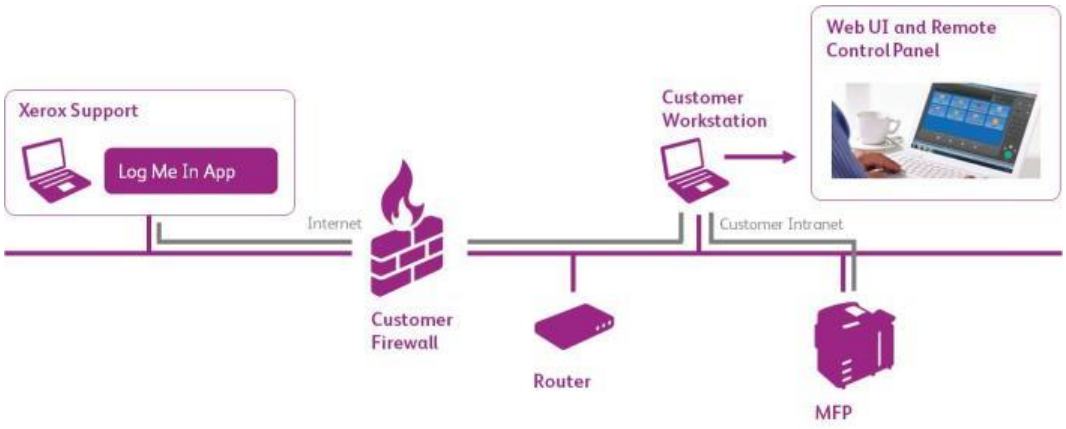
Since CSE's can access the inner workings of the software such as NVM writes, calibrations and specific routines, inadvertent key presses at the local UI could damage the device or require an on-site service visit. The CSE has the ability to block local control panel interaction if planning to perform one of these operations.

Any local physical interaction is subject to the device interlock system and may impede the service procedure but not expose the user to additional risks. Remote Control Panel has no ability to penetrate a customer's network firewall and therefore requires an assisted call utilizing a third-party remote session utility for physical interaction with the device. This helps assure that remote service calls will be locally attended and thus minimizes user collisions.

Local Service Safety

In this case, the service person is at the device performing a service action. Generally, a service person will disconnect the E-net cable at the start of the call so that remote jobs (print, fax, etc.) do not interrupt service procedures. However, this prevents the use of the remote UI for service collaboration. The feature does provide a method to enable the joint local and remote service action when desired, as in a collaboration call. The E-net cable must be plugged in and the remote person must authenticate in the Web UI with CSE credentials to connect the session. Any other user will be prevented from connecting via the Web UI if the device is in the service mode.

A CSE attempting to service the device on-site will need to be cognizant whether or not the device is in use, either locally or remotely. If the CSE approaches the machine with a remote session already activated, as signified by local UI status messages, the CSE will have to ensure the machine is free to use before starting to work on it. This is essentially no different than a CSE walking up to a machine and finding a user at it. The CSE waits until the user is done or asks them to stop what they are doing. CSEs will just continue to use their existing procedures and etiquette for access to the device. The final safeguard is that a remote session can always be terminated at the device by forcing the machine into power saver, rebooting it, or simply by unplugging the E-net cable.



Off-LAN access to device on customer's network via a third-party access tool.

Service Access to Customer Machine

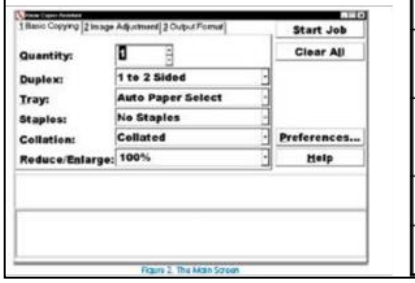
MFP devices are generally connected inside the customer's network and not exposed beyond their firewall. A typical service connection will require another application tool to access the machine through the firewall and will require customer SA assistance. These tools require the customer to "invite-in" the CSE to establish the connection and can be severed anytime by the customer. The diagram above shows how service would utilize a third party remote desktop access tool such as LogMeIn to access the device.

Generally the customer would call for service and be instructed how to start a remote session between their workstation and Xerox service. Once connected, the LogMeIn tool gives the service representative control of the client workstation in order to use it as a proxy from which to launch and control the device Web UI and Remote Control Panel.

The ability to collaborate through the customer's firewall is not built natively into the device, as these third-party tools are currently in use within the Xerox support infrastructure and have performed exceedingly well. Keeping this connection separate from the device also provides another level of security abstraction by eliminating another pathway into the device with its associated vulnerabilities.

Section 7 – Section 508

Section 508 is an extension of the US federal government Rehabilitation Act, which requires Federal agencies to make their electronic and information technology (including MFP's) accessible to people with disabilities. The Remote Control Panel significantly enhances several aspects of the requirement and is meant to supplement the Xerox® Copier Assistant® (XCA).



	XCA	Remote Control Panel
Mobility Impairment - Accessibility	Yes	Yes
Visual Impairment - Text-to-speech, Screen Mag	Yes	No
Dexterity Impairment - Keyboard Navigation (tab, arrows etc)	Yes	No
Languages - Other than English	No	Yes
Services - Other than Copy	No	Yes

XCA Screens

The remote control panel essentially displays the device LCD video display simultaneously in two places, the local UI and the client workstation. This is a raster image free from graphic elements or structures therefore doesn't support text-to-speech or tabbing navigation. The area it does excel in is illustrated in the above graphic. Anything the device local UI can display will be displayed remotely.

Section 8 – Key System Requirements

IP protocol supported	IPv4 and IPv6	
System OS supported	Same Windows, Mac, Linux and Unix operating systems supported by the Web UI	
OS not supported	Mobile devices – e.g. Apple iOS®, Android™, BlackBerry®, Windows Mobile	
Supported Browsers	Microsoft Internet Explorer 7.0, 8.0, 9.0, 10.0 Mozilla® Firefox® 4.0, 5.0 and up Google Chrome™ 12 and up Opera™ 11 Apple Safari® 5	Must support Java Applets and have Java scripting enabled
Java	Oracles 1.4.2_x or greater Java runtime for IPv4. Oracles 1.6.x or greater for IPv6	

Author

Joe Seyfried, System Planning Manager, Xerox Corporation

XOGWP-19UC