

# United States Trade Agreements Act (TAA) Compliant Xerox Printers and MFPs

**Xerox has a dedicated commitment to keeping information safe and secure** by identifying potential vulnerabilities and proactively addressing them to limit risk. Below is a selection of Xerox TAA Compliant products and some of the commonly required security features and options available with each.

## US Trade Agreements Act (TAA) Compliant Xerox Products

Xerox Product	TAA Configurations	802.1x Capable	IPv6	FIPS 140-2	IP Filtering	IPSec	SNMPv3	Disk Image Overwrite	Section 508
<b>Color Printers</b>									
Phaser 6600	YDN	•	•		•	•	•	•	•
Phaser 6700	YN / YDN /YDT / YDX	•	•	•	•	•	•	•	•
Phaser 7500	YDN /YDT / YDX	•	•		•	•	•	•	•
Phaser 7800	YDN /YDX / YGX	•	•	•	•	•	•	•	•
ColorQube® 8570	YN / YDN /YDT	•	•		•	•	•	•	•
<b>Black-and-White Printers</b>									
Phaser 3600	YDN	•	•		•	•	•		•
Phaser 4620	YDNM	•	•		•	•	•	•	•
Phaser 5550	YN / YDN / YDT/ YNM	•	•		•	•	•	•	•
<b>Color Multifunction Printers (letter/legal)</b>									
ColorQube 8700	S/X/XF	•	•	•	•	•	•	•	•
ColorQube 8900	X	•	•	•	•	•	•	•	•
<b>Black-and-White Multifunction Printers (letter/legal)</b>									
WorkCentre® 3550	YX	•	•		•	•	•		•
Phaser 3635MFP	YXM	•			•	•	•	•	•
WorkCentre 4250	YSM	•	•		•	•	•	•	•
WorkCentre 4260	YSM /YDNM	•	•		•	•	•	•	•
<b>Advanced Multifunction Printers (letter/legal/tabloid)</b>									
WorkCentre 5300 Series	YXC / YCH	•	•	•	•	•	•	•	•
WorkCentre 5700 Series	YAPT	•	•	•	•	•	•	•	•
WorkCentre 7120 Series	YPT	•	•	•	•	•	•	•	•
WorkCentre 7500 Series	YP / YPH / YPT	•	•	•	•	•	•	•	•
WorkCentre 9300 Series	YPM2 / YPM3	•	•	•	•	•	•	•	•

TAA compliant configurations denote that the country of origin for the specified configuration of that printer or MFP complies with the requirements of the US Trade Agreements Act (TAA).

# US Trade Agreements Act (TAA) Compliant Xerox Products Security Features

## 802.1x Device Authentication

Xerox office devices implement the 802.1x standard. This allows the device to be authenticated on a network before the network will allow any network traffic to pass to or from the device. This stops rogue devices from infiltrating the network.

## IPv6

Internet Protocol version 6 (IPv6) is the next-generation Internet Layer protocol for internetworks and the Internet. IPv6 has been implemented on all major operating systems in use in commercial, business, and home consumer environments. Network security is integrated into the design of the IPv6 architecture. The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

## IPsec

Internet Protocol Security (IPsec) secures Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. IPsec can be used for protecting any application traffic across the internet.

## IP Filtering Feature

Internet Protocol (IP) Filtering provides a system administrator with a means of restricting access to the system to a specific set of IP addresses. This provides a first level of defense against unauthorized use of the system. Computers whose IP addresses are outside of the allowed set are Not permitted to print.

## SNMP v3

Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices. SNMPv3 is the current standard version of SNMP as of 2004.

SNMPv3 provides important security features:

- Message integrity to ensure that a packet has Not been tampered with in transit.
- Authentication to verify that the message is from a valid source.
- Encryption of packets to prevent sNoooping by an unauthorized source.

## Disk Image Overwrite

The Image Overwrite security option electronically shreds information stored on the hard disk of devices as part of routine job processing. Electronic erasure can be performed automatically at job completion or on demand. The Xerox Image Overwrite security process implements a three-pass algorithm originally specified by the U.S. Department of Defense.

## Section 508

Section 508 of the Rehabilitation Act of 1973 requires Federal agencies to ensure their procurement of electronic and information technology takes into account the needs of all end users — including people with disabilities. Xerox has a long history of engineering products that are easy to access and operate. We have taken seriously our compliance with Section 508 requirements and have developed a rigorous process for assessing product compliance.

For more information, go to [www.xerox.com/security](http://www.xerox.com/security).

