Microsoft® Windows® 98 Resource Kit

A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Cataloging-in-Publication Data
Microsoft Windows 98 Resource Kit / Microsoft Corporation.
p. cm.
Includes index.
ISBN 1-57231-644-6
1. Microsoft Windows (Computer file) 2. Operating systems (Computers) I. Microsoft Corporation.
QA76.76.063M5244 1998
005.4'469--dc21 98-2768
CIP

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 WCWC 3 2 1 0 9 8

Distributed in Canada by ITP Nelson, a division of Thomson Canada Limited.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at mspress.microsoft.com.

Acquisitions Editors: Casey D. Doyle, David Clark, Anne Hamilton
Project Editor: Maureen Williams Zimmerman

This chapter presents an overview of security features provided in Microsoft Windows 98. It describes their use, together with security features of Internet Explorer version 4.0, in a networking environment. It is intended for system administrators and others who have authority to set security levels for network clients, and for those who need secure communication over the Internet.

In This Chapter

Overview of Security Features 356
Security Planning Checklist 360
Network Security 361
Passwords 370
Internet Explorer Security 376
Security Features in Outlook Express 383
Firewalls 388
Distributed Component Object Model 390
Troubleshooting Security 393

See Also

- For information about file and printer sharing services and user-level or share-level security, see Chapter 18, "Logon, Browsing, and Resource Sharing."
- For information about editing system policies, see Chapter 8, "System Policies."
- For information about security for Internet Explorer, see Chapter 20, "Internet Access and Tools."
- For information about Distributed Component Object Model (DCOM), see Chapter 29, "Windows 98 Network Architecture" and Chapter 25, "Application Support."

Overview of Security Features

Computer security refers to the protection of all components—hardware, software, and stored data—of a computer or a group of computers from damage, theft, or unauthorized use. A computer security plan that is well thought out, implemented, and monitored makes authorized computer use easy and unauthorized use or accidental damage difficult or impossible.

Personal computing depends increasingly on computers connected through networks, and more often through the Internet and intranets. You can use Windows 98 security to prevent unauthorized access to shared resources on computers in a network. The security features built into Windows 98 are described briefly in this section, and in more detail later in the chapter.

Logon Security

Windows 98 allows users to log on fully. In a networking environment, you can set your system up so that when a name and password pair have been validated against the security authority of a network server, the Windows 98 user interface is displayed.

Logon Password

A user can log on to all networks and Windows 98 at the same time. If a user's password for Windows 98 or for another network is the same as the password for the primary logon client, Windows 98 automatically logs the user on to Windows 98 and all networks using that password.

Note A unified password prompt does not enhance security, but eases logging on to the system. As the system administrator, you can require additional passwords for a more secure system.

For more information about the logon prompt, see "Using the Windows 98 Logon Password" later in this chapter. Once users log on to their machines, they have the option to cache their passwords. These passwords are cached in a file with a .pwl extension. The file name is the same as the user's name. See "Password Caching" later in this chapter.

Network Validation

With system policies, you can prevent users from logging on to Windows 98 if their Windows NT or Novell NetWare network logon is not validated. This causes the network logon dialog to appear before, or instead of, the Windows 98 logon prompt. Also, the user list may not be network wide, but specific to a server, and may be different for different servers.

Shared-Resource Security

When a computer is running Windows 98 with file and printer sharing services, other users can connect to shared printers, volumes, directories, and CD-ROM drives on that computer. To protect these shared resources, Windows 98 provides user-level and share-level security.

User-Level Security

With user-level security, a user's request to access a shared resource is passed through to a security provider, such as a Windows NT or NetWare server. The security provider grants or denies the request by checking the requestor's user name and password against a network-wide or server-wide stored list. User-level security does not require file and printer sharing services. These accounts must be created on the machine providing user-level authentication, such as a Windows NT or NetWare server. Windows 98 cannot act as an authentication server for user-level security.

This type of security allows fine-grained control over per-user access and allows individual accountability. The disadvantages are that you must create a user account for each user you want to grant access to, and you must grant that user the access.

Share-Level Security

With share-level security, users assign passwords to their shared resources. Any user who can provide the correct password is permitted to access the shared resource. The password is stored and checked by the computer where the resource resides. Share-level security requires file and printer sharing services.

Note Any subfolders of the shared folder, if they are also shared, must be set with the same level of security as the parent folder.

The advantage of this type of security paradigm is that it allows granting access to a broad range of people with very little effort. However, it is not as secure as user-level security, because the password is widely distributed and there is no notion of personal accountability.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.