



Reset User Password

Virtual Desktop Service

Toby vanRoojen
January 05, 2021

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Management.User_Administration.reset_user_password.html on July 20, 2021. Always check docs.netapp.com for the latest.

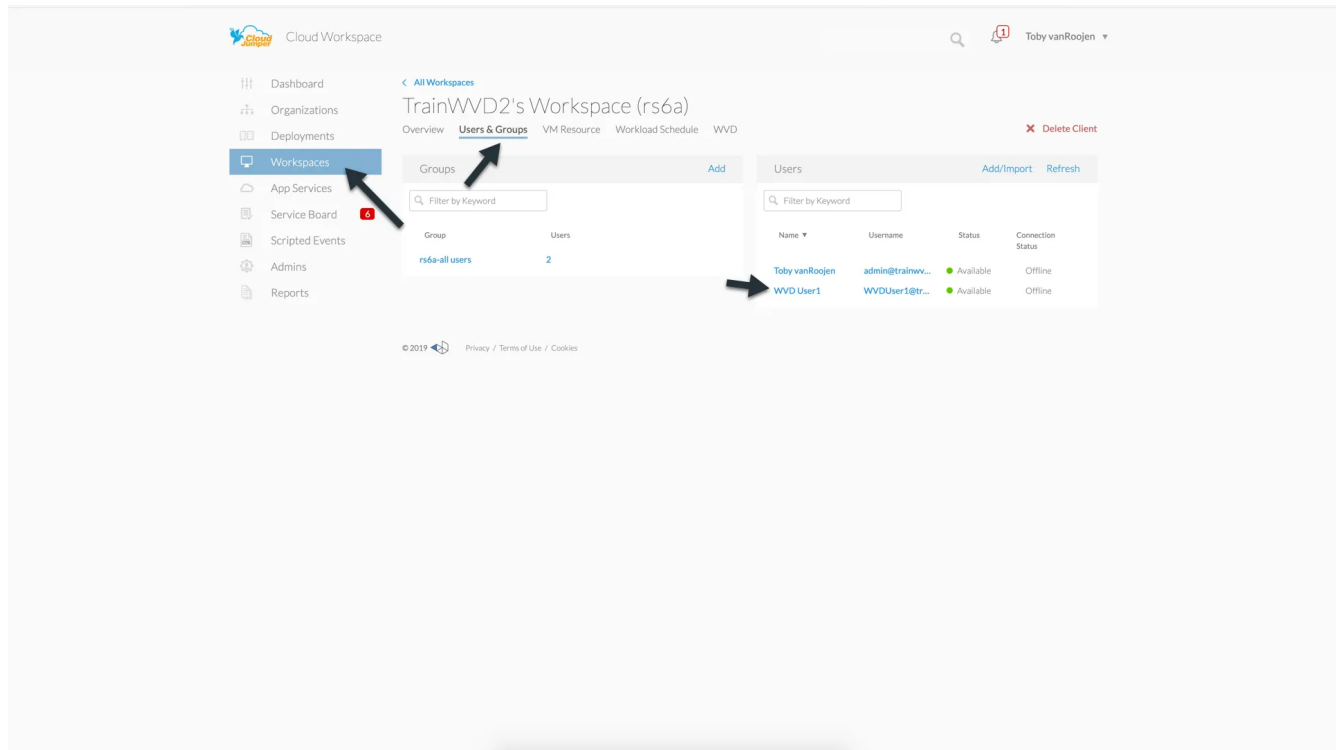
Table of Contents

- Reset User Password. 1
 - Reset user password steps 1
 - Time to take effect 2
- Self service password reset (SSRP) 3
- Password complexity 13

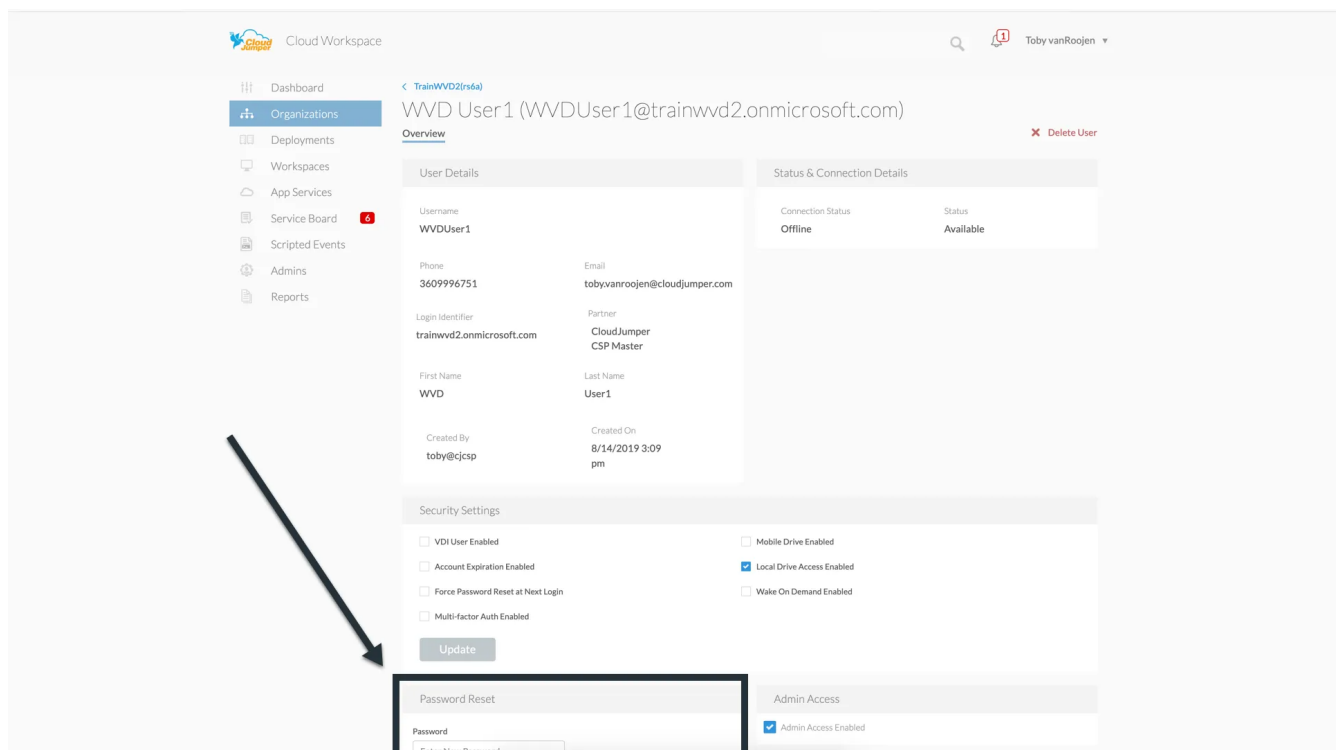
Reset User Password

Reset user password steps

1. Navigate to the Used Detail page in VDS



2. Find the Password Section, enter the new PW twice and click



First Name

WVD

Last Name

User1

Created By

toby@cjcsip

Created On

8/14/2019 3:09 pm

Security Settings

☐ VDI User Enabled
 ☐ Mobile Drive Enabled

☐ Account Expiration Enabled
 ☒ Local Drive Access Enabled

☐ Force Password Reset at Next Login
 ☐ Wake On Demand Enabled

☐ Multi-factor Auth Enabled

Update

Password Reset

Password

Confirm Password

Reset Password

Admin Access

☒ Admin Access Enabled

Applications

☒ Application
 ☒ 7zip - Current Version (v. Latest)
 ☐ Calculator

Group Policy

No

No

Update

Processes

No Processes Running.

© 2019 Privacy / Terms of Use / Cookies

Time to take effect

- For environments running an “Internal” AD on VMs in the environment the password change should take effect immediately.
- For environments running Azure AD Domain Services (AADDs) the password change should take about 20 minutes to take effect.
- The AD type can be determined on the Deployment Details Page:

Cloud Workspace

Dashboard

Organizations

Deployments

Workspaces

App Services

Service Board

Scripted Events

Admins

Reports

< All Deployments

trainwvd2.onmicrosoft.com (kjd)

Overview Resource Defaults Backup Defaults Provisioning Collections

Deployment Details

Microsoft Azure

Description

trainwvd2.onmicrosoft.com

Version

5.3

Resource Allocation Type

MachineSize

h5 Gateway

kjd-h5gw.kjd.cloudworkspace.app:444

FTP Server Address

kjd-ftp.kjd.cloudworkspace.app

Deployment Code

kjd

Hypervisor

Azure

Domain

trainwvd2.onmicrosoft.com

RDP Gateway

kjd-rds.kjd.cloudworkspace.app

Directory Type

AADDs

Workloads

Workspaces 1

App Services

Profile Server

☐ Enabled

Platform Servers

Refresh

Name	CPU	RAM (GB)	Status
CWMGR1	2	4	Online

Platform Processes

Refresh

New Client	Idle	New User	Idle	New App Service	Idle
Update Client	Idle	Update User	Idle	Update App Service	Idle
Delete Client	Idle	Delete User	Idle	Delete App Service	Idle
Server Cache	Idle				

Self service password reset (SSRP)

The NetApp VDS Windows client and the NetApp VDS web client will provide a prompt for users that enter an incorrect password when logging into a v5.2 (or later) virtual desktop deployment. In the event that the user has locked their account, this process will unlock a user's account as well.

Note: users must have already entered a mobile phone number or an email address for this process to work.

SSPR is supported with:


- NetApp VDS Window Client
- NetApp VDS Web Client

In this set of instructions, you will walk through the process of using SSPR as a simple means to enable users to reset their passwords and unlock their accounts.

NetApp VDS Windows client

1. As an end user, click the Forgot Password link to continue.

CloudJumper | Cloud Workspace®



Welcome to Cloud Workspace®
Sign into your workspace

Please check your username and password and try again.

Username

recording@wvdrecording.onmicrosoft.com

Password

●●●●●●●●

[Forgot Password](#)


Save Username

☐

Sign In

2. Select whether to receive your code via your mobile phone or via email.

CloudJumper | Cloud Workspace®



Welcome to Cloud Workspace®

Sign into your workspace

Username

recording@wvdrecording.onmicrosoft.com

Send Code Using:

Email

Email

Phone

Request Code

Cancel

3. If an end user has only provided one of those contact methods, that will be the only method displayed.

CloudJumper | Cloud Workspace®

CloudJumper

Welcome to Cloud Workspace®

Sign into your workspace

Username

recording@wvdrecording.onmicrosoft.com

Send Code Using: Phone

Request Code Cancel

4. After this step, users will be presented with a Code field where they should enter the numeric value received either on their mobile device or in their inbox (depending which was selected). Enter that code followed by the new password and click Reset to proceed.

The screenshot shows the CloudJumper Cloud Workspace login window. At the top, the title bar reads 'CloudJumper | Cloud Workspace®' with standard window controls. The main header area is dark blue with the CloudJumper logo (a stylized cloud with a bird-like shape) and the text 'Welcome to Cloud Workspace®' and 'Sign into your workspace'. Below this, the login form is on a light gray background. It includes fields for 'Username' (containing 'recording@wvdrecording.onmicrosoft.com'), 'Code' (containing '975365'), 'New Password' (masked with dots), and 'Confirm Password' (masked with dots and a cursor). At the bottom are 'Reset' and 'Cancel' buttons.

5. Users will see a prompt informing them that their password reset has been completed successfully – click Done to proceed to complete the login process.




If your deployment is using Azure Active Directory Domain Services, there is a Microsoft-defined password sync period – every 20 minutes. Again, this is controlled by Microsoft and cannot be changed. With this in mind, VDS displays that the user should wait for up to 20 minutes for their new password to take effect. If your deployment is not using Azure Active Directory Domain Services, the user will be able to log in again in seconds.

CloudJumper | Cloud Workspace®

—

×



Welcome to Cloud Workspace®
Sign into your workspace

Your password has been reset successfully.
Please allow up to 20 minutes before using the new password to login.

Username

recording@wvdrecording.onmicrosoft.com

Code

975365

New Password

Confirm Password

●●●●●●●●

●●●●●●●●

Reset

Done

HTML5 portal

1. If the user fails to enter the correct password when attempting to login through the HTML5, they will now be presented with an option to reset the password:

A login form on a dark blue background. It features a white input field for the username containing 'demo@cloudjumper' and a white input field for the password with four dots. Below the fields, a message reads: 'The username or password is incorrect. Click [HERE](#) if you need to reset your password.' At the bottom is a blue button labeled 'LOG IN'.

2. After clicking on the option to reset their password, they will be presented with their reset options:

A form for password reset options on a dark blue background. It has a white input field for the email address containing 'demo@cloudjumper'. Below it are two radio buttons: 'Email' (unselected) and 'SMS' (selected). At the bottom are two blue buttons labeled 'REQUEST' and 'CANCEL'.

3. The 'Request' button will send a generated code to the option selected (in this case the user's email). The code is valid for 15 minutes.

A form for entering the reset code and new password on a dark blue background. It includes a white input field for the email address containing 'demo@cloudjumper', two radio buttons for 'Email' (unselected) and 'SMS' (selected), a white input field for a code containing '882974', and two white password input fields with dots. Below the fields, a message reads: 'Please enter the code you received and a new password.' At the bottom are two blue buttons labeled 'SUBMIT' and 'CANCEL'.

4. The password has now been reset! It is important to remember that Windows Active Directory will often need a moment to propagate the change so if the new password does not work immediately, just wait a few minutes and try again. This is particularly relevant for users residing in an Azure Active Directory Domain Services deployment, where a password reset could take up to 20 minutes to propagate.



The image shows a dark blue dialog box with white text and input fields. At the top, there is a user icon and the email address 'demo@cloudjumper'. Below this are two radio buttons labeled 'Email' and 'SMS'. Under the 'SMS' button, there is a field with a hash symbol and the number '882974'. Below that are two password fields, each with a key icon and ten dots representing masked characters. At the bottom, there is a message: 'Your password has been reset. If it does not work immediately, please wait a few minutes and try again.' and a blue 'OK' button.

Enabling self service password reset (SSPR) for users

To use Self Service Password Reset (SSPR), administrators must first enter a mobile phone number and/or an email account for an end user. There are two ways to enter a mobile number and email addresses for a virtual desktop user as detailed below.

In this set of instructions, you will walk through the process of configuring SSPR as a simple means for end users to reset their passwords.

Bulk importing users via VDS

Start by navigating to the Workspaces module, then Users & Groups and then clicking Add/Import.

You can enter these values for users when creating them one by one:

Or you can include these when bulk-importing users downloading and uploading the preconfigured Excel XLSX file in with this content filled out:

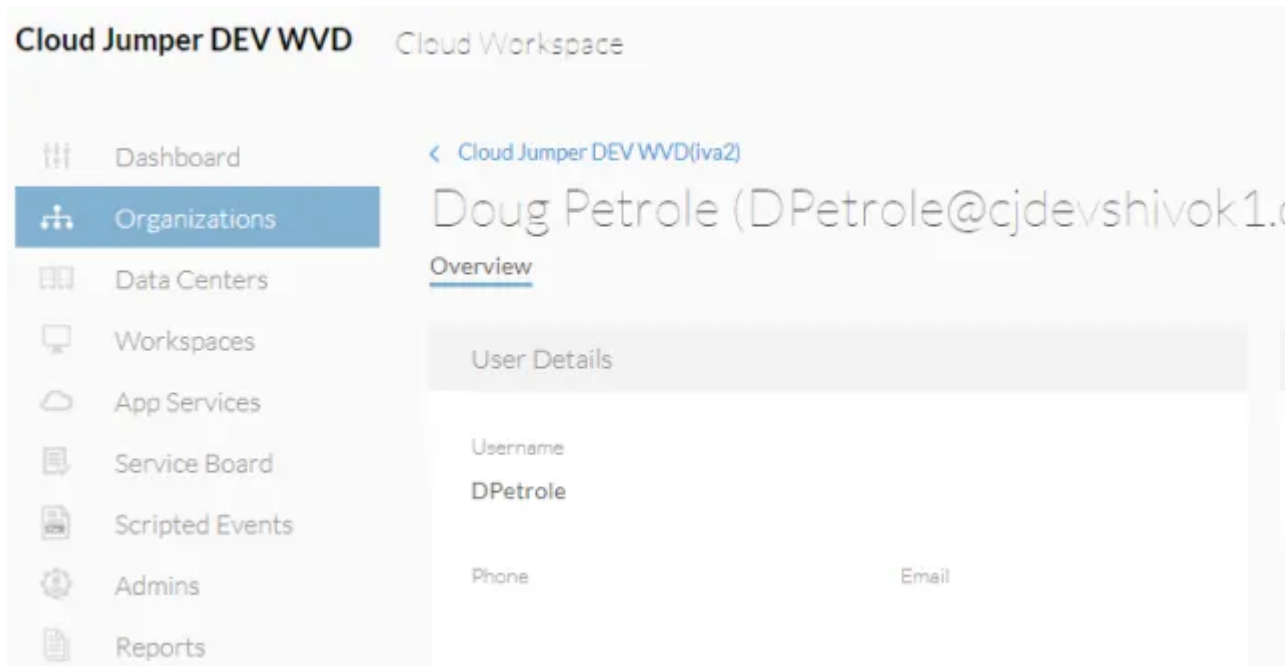
The screenshot shows the top portion of a Microsoft Excel window. The title bar at the top indicates the file name "user-upload-template-3d781dba62 - Protected View - Excel" and lists several open documents, including "Doug Petrole". Below the title bar is the ribbon menu, which includes tabs for File, Home, Insert, Draw, Page Layout, Formulas, Data, Review, View, Help, Acrobat, and Tell me. A yellow banner across the top of the worksheet area displays a message: "PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View." Below this banner is the formula bar, which currently shows "E2" in the Name Box and contains icons for undo, redo, and insert functions. The main grid of the spreadsheet is visible, with columns labeled A through J and rows numbered 1 through 7. Column E is highlighted, and its header cell "Phone Number" is selected. The other cells in the first row are labeled "First Name", "Last Name", "Login", and "Email".

Supplying the data via the VDS API

NetApp VDS API – specifically this call https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – provides the ability to update this information.

Updating existing user phone

Update the users' phone number on the User Detail Overview page in VDS.



Using other consoles

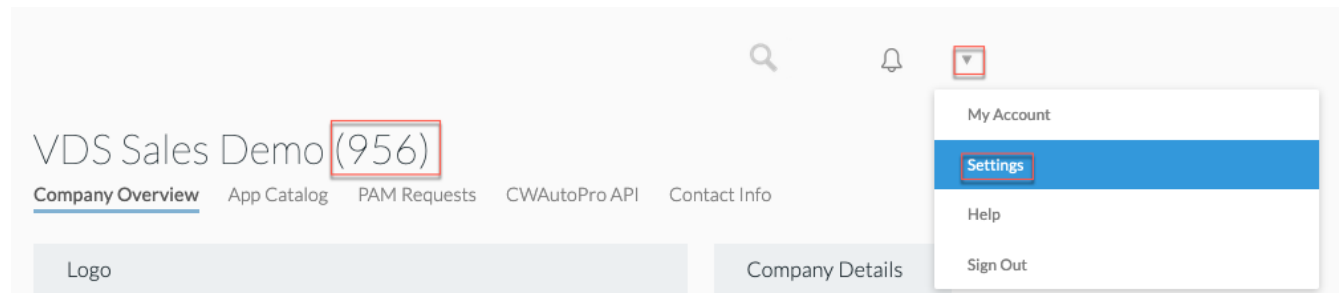
Note: you currently cannot provide a phone number for a user via the Azure Console, Partner Center or from the Office 365 Admin console.

Customize SSPR sending address

NetApp VDS can be configured to send the confirmation email *from* a custom address. This is a service provided to our service provider partners who wish for their end users to receive the reset password email to be sent from their own customized email domain.

This customization requires some additional steps to verify the sending address. To start this process, please open a support case with VDS support requesting a custom "Self Service Password Reset Source Address". Please define the following:

- Your partner code (this can be found by clicking on *settings* under the upper-right down arrow menu. See screenshot below)



- Desired "from" address (which must be valid)
- To which clients the setting should apply (or all)

Opening a support case can be done by emailing: VDSsupport@netapp.com

Once received, VDS support will work to validate the address with our SMTP service and activate this setting. Ideally you'll have the ability to update public DNS records on the source address domain to maximize email deliverability.

Password complexity

VDS can be configured to enforce password complexity. The setting for this is on the Workspace Detail Page in the Cloud Workspace Settings section.

Scroll down

The screenshot displays the 'TrainWVD2's Workspace (rs6a)' detail page. The left sidebar contains a navigation menu with 'Workspaces' highlighted. The main content area features two line graphs: 'Active Users' and 'Resource Consumption'. Below the graphs are sections for 'Deployment', 'App Services', 'Company Details', and 'Contact Details'. The 'Company Details' section includes fields for Company Name, Company Code, Status, Organization Type, Client, and Created By. The 'Contact Details' section includes fields for Primary Notification Email, Phone, Address 1, Address 2, City, Zip Code, State, and Country.

The screenshot displays the 'CloudJumper CSP Master' configuration interface. The 'Cloud Workspace Settings' section is highlighted, showing various settings categorized into App, Device, and Security. The 'Force Password Complexity' checkbox under Security Settings is checked. Other settings include Remote App Access, Enable Application Usage Tracking, Disable Printing Access, User Profile Disk, User Data Storage, Enable Task Manager, File Auditing Enabled, Migration Mode Enabled, and MFA for All Users Enabled. The 'Update' button is visible at the bottom of the settings section. The 'Account Options' section shows 'Account Lockout Notifications' as unchecked. The 'Audit Reports' section has a dropdown menu for selecting a report. The 'Apps' section includes a search bar and a list of installed applications.

Password complexity: Off

Policy	Guideline
Minimum Password Length	8 characters
Maximum Password Age	110 days
Minimum Password Age	0 days
Enforce Password History	24 passwords remembered
Password Lock	Automatically lockout will occur after 5 incorrect entries
Lock Duration	30 minutes

Password complexity: On

Policy	Guideline
Minimum Password Length	<p>8 characters</p> <p>Not contain the user's account name or parts of the user's full name that exceed two consecutive characters</p> <p>Contain characters from three of the following four categories:</p> <ul style="list-style-type: none"> English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, !, \$, #, %) <p>Complexity requirements are enforced when passwords are changed or created.</p>
Maximum Password Age	110 days

Policy	Guideline
Minimum Password Age	0 days
Enforce Password History	24 passwords remembered
Password Lock	Automatically lock will occur after 5 incorrect entries
Lock Duration	Remains locked until administrator unlocks

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.