Dell Remote Access Configuration Tool for Microsoft Windows Operating Systems

Version 1.1 User's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Information in this publication is subject to change without notice.

Trademarks used in this text: Dell™, the Dell logo, Dell Precision™ , OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™ and Vostro™ are trademarks of Dell Inc. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS® and Windows Vista® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

2012 - 03

Rev. A00

Contents

1

Introducing Dell Remote Access Configuration Tool

Dell Remote Access Configuration Tool (DRACT) discovers and configures Remote Access Controllers (RACs) for systems on your network from a single console. You can use this tool to perform the following:

- Discover or import RAC IP addresses on the network.
- Update firmware for selected RAC IP addresses.
- Configure standard or extended schema-based Active Directory (AD) settings for selected RAC IP addresses.
- Create RAC objects on the AD server for extended schema-based AD.

Supported RACs

DRACT supports the following types of RACs that support RACADM commands:

- Integrated Dell Remote Access Controller 7 (iDRAC7)
- Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for rack and tower servers
- Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for blade servers
- Chassis Management Controller (CMC)
- Dell Remote Access Controller 5 (DRAC 5)
- Dell Remote Access Controller 4 (DRAC 4)

Supported Operating System

You can install DRACT on 32-bit and 64-bit Microsoft Windows operating systems such as Windows XP, Windows Vista, Windows 7, and Windows Server 2008.

Before You Begin

Before using DRACT, make sure that you have performed the following to use the AD authentication feature:

- Deploy AD infrastructure. See the Microsoft website for information on how to set up an AD infrastructure.
- Setup the standard Public Key Infrastructure (PKI) mechanism. RACs use the PKI mechanism to authenticate securely into the AD; therefore, an integrated PKI into the AD infrastructure is required. See the Microsoft website for more information on the PKI setup.
- Enable the Secure Sockets Layer (SSL) on all domain controllers that the RAC connects to. This is required to correctly authenticate all the domain controllers. For more specific information, see "Enabling SSL on a Domain Controller" section in the appropriate RAC user guide listed in Other Documents You May Need.
- If you are planning to use extended schema-based AD authentication, extend your current AD schema to incorporate Dell Remote Access Controller classes and attributes using the AD setup package or *Dell Systems Management Tools and Documentation* DVD. For information about the AD setup package, see the readme file available with the package.

Other Documents You May Need

In addition to this guide, you can see the following guides on the Dell Support website at **support.dell.com/manuals** or use the direct link on the *Dell Systems Management Tools and Documentation* DVD.

- The *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide* provides information about configuring and using an iDRAC7 for rack, tower, and blade servers to remotely manage and monitor your system and its shared resources through a network.
- The *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers User Guide* provides information about configuring and using an iDRAC6 for blade servers to remotely manage and monitor your system and its shared resources through a network.
- The *Integrated Dell Remote Access Controller 6 (iDRAC6) User Guide* provides complete information about configuring and using an iDRAC6 for tower and rack servers to remotely manage and monitor your system and its shared resources through a network.
- The *Dell Remote Access Controller 5 Firmware User's Guide* provides complete information about installing and configuring a DRAC 5 controller and using DRAC 5 to remotely access an inoperable system.
- The *Dell Remote Access Controller 4 User's Guide* provides complete information about installing and configuring a DRAC 4 controller and using DRAC 4 to remotely access an inoperable system.
- The *Dell Chassis Management Controller (CMC) User's Guide* provides information about using the controller that manages all modules in the chassis containing your Dell PowerEdge server.
- The *Glossary* provides information about the terms used in this document.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit **support.dell.com**.
2. Select your support category.
3. If you are not a U.S. customer, select your country code at the bottom of the **support.dell.com** page, or select **All** to see more choices.
4. Select the appropriate service or support link based on your need.

2

Installing and Uninstalling DRACT

This section provides information about how to install and set up DRACT on your system.

Prerequisites

The prerequisites to install and run DRACT on your system are:

- Install .Net Framework version 2.0 SP1 (or later).
- Download the DRACT installer file (**.msi**) from the Dell Support website at **support.dell.com**.
- A user account with installation and execution privileges.

Installing DRACT

You can install DRACT in one of the following ways:

- Using DRACT installer (**.msi**) file
- Using Command Line Interface (CLI)
- Using Active Directory (AD) Setup Package

Installing DRACT Using MSI Installer

To install DRACT:

1. Double-click the DRACT installer (**.msi**) file.
   The **Welcome to the Dell Remote Access Configuration Tool Setup** wizard is displayed.
2. Click **Next**.
   The **License Agreement** window is displayed.
3. Select **I Agree** and click **Next**.
   The **Select Installation Folder** window is displayed.
4. Click **Browse** and select the folder where the software must be installed.
   By default, the folder is **C:\Program Files\Dell\RACT**. You can click **Disk Cost** to view the available and required disk space for each drive.
5. Select one of the following user access options:
   - **Everyone** - Install the software for anyone who uses the system
   - **Just me** - Install the software for the current user account
6. Click **Next**.
   The **Confirm Installation** window is displayed.
7. Click **Next** to start the installation.
   After the installation is complete, the **Installation Complete** window is displayed.
8. Click **Close** to exit the application.

Installing DRACT Using CLI

To install DRACT using CLI:

1. Run the command `msiexec /I <path>/<package name>.msi` at the command prompt, where, <path> is the location of the DRACT installer file and <package name> is the DRACT installer name.

   The **Welcome** window is displayed.
2. Perform the steps provided in Installing DRACT Using MSI Installer.

Installing DRACT Using AD Setup Package

You can install DRACT using the AD Setup Package. For more information, see the **readme.txt** file available on the Dell Support website at **support.dell.com/manuals**.

Launching DRACT

You can launch DRACT in one of the following ways:

- Go to **Start** → **Programs** → **Dell** → **Remote Access Configuration Tool**. The **Welcome** window is displayed.
- On your desktop, double-click the **Dell Remote Access Configuration Tool** icon. The **Welcome** window is displayed.

Uninstalling DRACT

You can uninstall DRACT in one of the following ways:

- Using DRACT installer (.msi) file
- Using Control Panel
- Using CLI

Uninstalling DRACT Using MSI Installer

Make sure that you have the DRACT installer file on your system. If you do not have the installer file, you can download it from the Dell Support website at **support.dell.com**.

To uninstall DRACT:

1. Double-click the DRACT installer (**.msi**) file.

   The **Welcome to Dell Remote Access Configuration Tool Setup Wizard** is displayed.
2. Select the **Remove Dell Remote Access Configuration Tool** option and click **Finish**.

   The **Removing Dell Remote Access Configuration Tool** window displays the status bar. After the DRACT tool is uninstalled, the **Installation Complete** window displays the message "Dell Remote Access Configuration Tool has been successfully removed."
3. Click **Close** to exit.

Uninstalling DRACT Using Control Panel

To uninstall DRACT:

1. Go to **Start** → **Control Panel** → **Add or Remove Programs** .
2. Select **Dell Remote Access Configuration Tool** and click **Remove**.

   After DRACT is uninstalled, it is removed from the list.

Uninstalling DRACT Using CLI

To uninstall DRACT using CLI:

1. Run the command `msiexec /x <path>/<package name>.msi` at the command prompt, where, <path> is the location of the DRACT installer file and <package name> is the DRACT installer name.

   The **Welcome** window is displayed.
2. Perform the steps provided in “Uninstalling DRACT Using MSI Installer”.

Log File

A log file is created and is available to you after you close the application. The log file logs events, and contains details of firmware update and configuration for each RAC. The log file is updated each time you use DRACT.

The log file is available in the **C:\temp** folder.

NOTE: The log file is created only if the **C:\temp** folder is available.

3

Discovering Importing and Verifying RACs

Firmware updates or configuring RACs requires discovery and verification of the RACs on the network. You can use DRACT to discover the RAC IP addresses or import a **.csv** file containing the RAC IP addresses that are discovered, and append the imported list of RAC IP addresses to the existing list.

You can specify the RAC types you need to discover for a specific IP address or a range of IP addresses.

After discovering the RAC IP addresses on your network, you must verify that you have the required permissions to update firmware or configure the RACs using login credentials that is common for all the discovered RAC IP addresses.

You can perform the following:

- Discover RAC IP addresses on your network.
- Import a **.csv** file that contains a list of discovered RAC IP addresses.
- Perform a discovery and then import a **.csv** file. The imported list of RAC IP addresses is appended to the existing list.

Discovering RACs

To discover RAC IP addresses on your network:

1. Launch DRACT.

   The **Welcome** window is displayed. For information to launch DRACT, see Launching DRACT.
2. Click **Next**.

   The **Discover or Import Remote Access Controllers** window is displayed.
3. In the text box, specify the IP addresses separated by a comma, or a range of IP addresses using a hyphen.

   You can use '*' in the fourth field, for example, 10.94.20.34, 10.94.22.*, 10.94.20.100-200.
4. Select one or more of the following options to specify the RAC types that you want to discover:

   – iDRAC7
   – iDRAC6 for Racks and Towers
   – iDRAC6 for Blade Servers
   – CMC
   – DRAC5
   – DRAC4
5. Click **Discover**.

   The discovered IP addresses along with the RAC type and the status information is displayed; the status in the **Status** column is **Discovered**. After all the RAC IP addresses are discovered, the message "Completed discovery of Remote Access Controllers" is displayed.
6. Click **OK** to continue.

   Once the RAC IPs are displayed, you can click on a RAC IP address link to launch the web-based Graphical User Interface (GUI). To sort the entries in ascending or descending order for each column, you can click on the column heading.

Importing RACs

If you have a list of discovered RAC IP addresses saved in a **.csv** file, you can import the file into DRACT or you can perform a discovery and then import the **.csv** file. The contents of the file are appended to the existing list of discovered RAC IP addresses.

To import a list of RAC IP addresses:

1. Launch DRACT. For information on the steps, see Launching DRACT.

   The **Welcome** window is displayed.
2. Click **Next**.

   The **Discover or Import Remote Access Controllers** window is displayed.
3. Click **Import**.

   The **Import Remote Access Controllers** dialog box is displayed.
4. Select the **.csv** file that has the list of RAC IP addresses that are discovered and click **Open**.

   The contents of the **.csv** file are extracted and displayed in the **Discover or Import Remote Access Controllers** window.
5. Click **Next**.

   The **Verify Remote Access Controllers** window is displayed. For information about verifying RACs, see Verifying RACs.

Verifying RACs

After the discovery or import of RAC IP addresses is complete, verify that you have the required permission by providing a user name and password valid for all the RACs; either the local RAC or AD login credentials. User permissions must be verified before performing firmware updates or RAC configuration.

Enter the following in the **Verify Remote Access Controllers** window:

1. In the **User Name** field, enter a user name.
2. In the **Password** field, enter a password.

NOTE: The user name and password you provide must have configuration privileges on the RACs.

3. Select any or all of the following options to filter the discovered RACs based on the RAC type you must verify:

   – iDRAC7
   – iDRAC6 for Racks and Towers
   – iDRAC6 for Blades
   – CMC
   – DRAC5
   – DRAC4

   When you select a RAC type, the corresponding RAC IP addresses are selected from the list. You can also select individual RAC IP addresses from the list.
4. Click **Verify**.

   Based on the success or failure of the operation, the **Status** column displays the following messages for each IP address:

   – Verifying
   – Verified

  - Verification Failed
  - Access Denied
  - A required license is missing or expired

NOTE: If the **Status** is Verified, the DNS name and firmware version is also displayed.

After all the RAC IP addresses are verified, the "Verification of the selected RACs is completed." message is displayed.

5. Click **OK**.

   This completes the verification process.

NOTE: You can click **Export** and save the list of RAC IP addresses as a **.csv** file. You can import this **.csv** into DRACT at a later time to perform a verification.

6. Click **Next**.

   The **Firmware update configuration** window is displayed.

7. Click **OK** to delete the IP addresses.

   The **Firmware Update Configuration** window is displayed. For information about updating firmware, see Updating RAC Firmware.

4

Updating RAC Firmware

After you have discovered and verified the RAC IP addresses on your network, you can perform a firmware update on the selected RACs using the firmware image file located on your local directory or on the Trivial File Transfer Protocol (TFTP) server. For information to discover and verify RAC IP addresses, see Discovering Importing and Verifying RACs.

NOTE: iDRAC6 Enterprise for blade servers (version 3.3 and later) supports firmware update using the local directory. All the other DRAC types including iDRAC7 are also supported.

All firmware image files for different RACs must reside in the same folder. The DRACT tool uses the correct firmware image file based on the file name extension. Currently, all RACs have different image file name extensions based on the RAC type. The file name extensions are:

- iDRAC7 — **firming.d7**
- iDRAC6 for rack and tower servers — **firmimg.d6**
- iDRAC6 for blade servers — **firmimg.imc**
- CMC — **firmimg.cmc**
- DRAC5 — **firmimg.d5**
- DRAC4 — **firmimg.dm1**

NOTE: Only the default file names are accepted and other file names are not recognized. Make sure that you do not change the default file names.

To update RAC firmware:

1. Discover and verify the RAC IP addresses on your network. For more information, see Discovering Importing and Verifying RACs.
2. In the **Firmware Update Configuration** window, under **Specify Firmware Location**, select one of the following options to specify the location of the firmware image files:
   - **From TFTP Server** — Enter the location on the TFTP server where the firmware image files are stored. If the image files are stored at the root, enter only the IP address. If the image files are stored in a folder, enter the IP address and the path.
   - **From Local Directory** — Click **Browse** and specify the location of the firmware image files on your local directory.
3. Select any or all of the following options to select the RACs to update firmware:
   - iDRAC7
   - iDRAC6 for Racks and Towers
   - iDRAC6 for Blades
   - CMC
   - DRAC5
   - DRAC4

     When you select a RAC type, the corresponding RAC IP addresses are selected from the list. You can also select individual RAC IP addresses from the list.

In the firmware image file folder, if there is no firmware image file for a specific RAC type, then the corresponding option is disabled and is not available for selection. For example, if the firmware image file is not available for DRAC 4, then you cannot select the **DRAC4** option.

4. Click **Update Firmware**.

   If the firmware update is successful, the **Status** column displays the following messages in a sequence for each IP address:

   - Preparing Firmware Update
   - Transferring Firmware Image — This message is displayed only when the firmware image files are used from your local directory location.
   - Updating Firmware
   - Restarting
   - Firmware Update Success

   If the firmware update is not complete, the **Status** column displays one of the following messages for the IP address(es):

   - Failed to initiate
   - Insufficient Privileges
   - Unable to find Firmware image
   - Firmware Update Failed

   For information on the reasons for failure and the solution, see Troubleshooting and Frequently Asked Questions.

   After the firmware is updated for the selected RACs, the "Firmware Update Completed" message is displayed.

5. Click **OK** to complete the firmware update for the selected RACs.

5

Configuring RACs Using Microsoft Active Directory

The Active Directory (AD) service maintains a common database of all information needed for controlling users on a network. If you are using the AD software, you can configure it to provide access to the RACs, allowing you to add and control user privileges for the existing users in your directory service.

AD centralizes all RAC user IDs and passwords using standard or extended schema. Standard schema uses AD group objects only, and extended schema uses Dell-defined AD objects. When using AD to configure RAC access, you must choose standard or extended schema. For more information on standard and extended schema, see the appropriate RAC user guide listed in Other Documents You May Need.

Using DRACT, you can perform the following actions for selected RACs on your network:

- Configure standard or extended schema based AD settings for selected RACs.
- Create RAC objects on AD server for extended schema-based AD.

NOTE: Before you connect the AD server to DRACT, make sure that your AD server is configured to communicate with the RAC. For more information, see the appropriate RAC user guide listed in Other Documents You May Need.

You can upload the digital certificate used during the initiation of the Secure Sockets Layer (SSL) connections when communicating with an AD server; these communications use LDAP over SSL (LDAPS).

If certificate validation is enabled, it is necessary to upload the certificate of the Certificate Authority (CA) that issued the AD server certificate during initiation of SSL connections. The CA certificate is used to validate the authenticity of the certificate provided by the AD server during SSL initiation. The AD CA Certificate is the certificate that signs all the domain controllers' SSL server certificates.

NOTE: Uploading a CA certificate is optional for iDRAC6 and iDRAC7, but mandatory for DRAC 4, DRAC 5, and CMC. The AD CA certificate that is being uploaded must be the same certificate that is on the AD server. For iDRAC6 and iDRAC7, if the certificate is not specified, the default SSL certificate is used

Using DRACT, you can perform the following configurations for RACs that are configured to a standard schema, extended schema, or for RACs that have AD schema disabled:

- Configure RACs using AD standard schema. For more information, see Configuring RACs Using AD Standard Schema.
- Configure RACs using AD extended schema. For more information, see Creating RAC objects and Configuring RACs Using AD Extended Schema.
- Disable AD standard or extended schema for RACs. For more information, see Disabling AD Standard or Extended Schema for RACs.

Configuring RACs Using AD Standard Schema

In standard schema, a standard group object is used as a role group on the AD server. A user who has access to RACs is a member of the role group. To provide access to a specific RAC for this user, the role group name and its domain name must be configured on the specific RAC. You must specify an existing role group name available on the AD server. The role and the privilege level is defined on each RAC. You can define and configure up to five role groups. For more information on standard schema, see the appropriate RAC user guide listed in Other Documents You May Need.

To configure RACs using AD standard schema settings:

1. Discover and verify the RAC IP addresses on your network. For more information, see Discovering Importing and Verifying RACs.
2. In the **Firmware Update Configuration** window, click **Next**.

   The **Active Directory Configuration** window is displayed. The **Schema** column indicates that the RAC is configured to a standard or extended schema. If it is not configured, the **Schema** column displays **Disabled**.
3. Under **Filter on Schema**, select one of the following filter options to select the RACs that you must configure:

   – Standard Schema

   – Extended Schema

   – Active Directory disable

     When you select a filter type, the corresponding RAC IP addresses are selected from the list. You can also select individual RAC IP addresses from the list.
4. Under **New Schema**, select **Standard Schema** and click **Next**.

   The **Common Settings** window is displayed. The settings in this window are common for both standard and extended schema.
5. In the **Common Settings** window, enter the following:

   – Under **Upload Active Directory CA certificate**, click **Browse** and select the CA certificate file to be uploaded.

NOTE: This is optional for iDRAC6 and iDRAC7, but mandatory for DRAC 4, DRAC 5, and CMC. The AD CA certificate that is being uploaded must be the same certificate that is on the AD server. For iDRAC6 and iDRAC7, if the certificate is not specified, the default SSL certificate is used.

   – If you have selected the RAC IP addresses for iDRAC6 or iDRAC7, click the **iDRAC6/iDRAC7** tab and enter the AD settings. For information about the settings, see *Dell Remote Access Configuration Tool Online Help*.

   – If you have selected the RAC IP addresses for DRAC4, DRAC5, or CMC, click the **DRAC4 / DRAC5 / CMC** tab and enter the AD settings. For information about the settings, see *Dell Remote Access Configuration Tool Online Help*.
6. Click **Next**.

   The **Standard Schema Settings** window is displayed.
7. Enter the standard schema settings for the RAC type. For information about the settings, see *Dell Remote Access Configuration Tool Online Help*.
8. Click **Apply**.

   The **Summary** window displays the following information for the selected RACs:

   – RAC IP address

   – DNS name

   – RAC Type

   – Firmware version

   – Status information

   – Status bar

     If the configuration is successful, the **Status** column displays the following messages in a sequence for each IP address:

     * Uploading CA certificate - This message is displayed only if you have enabled CA certificate validation.
     * Configuring - RAC configuration is in-progress.
     * Configuration Success - RAC configuration is successful.

If the configuration is not complete, the **Status** column displays one of the following messages for the IP address(es):

- Certificate Upload Failed - CA certificate uploaded is invalid.
- Configuration Failed - RAC configuration is not successful.
- Insufficient Privileges - The required privileges are not provided to configure the RAC.

For more information on the **Status** column messages, see Troubleshooting and Frequently Asked Questions.

After all the configurations are completed, the message "Done" is displayed.

9. Click **OK**. The standard schema settings are configured for the selected RAC IP addresses.

Creating RAC objects and Configuring RACs Using AD Extended Schema

Dell has extended the AD schema to include an association, device, and privilege property. The association property is used to link together the users or groups with a specific set of privileges to one or more RAC devices.

For each physical RAC on the network that you need to integrate with the AD server for authentication and authorization, it must have at least one association object and one RAC device object.

You need to specify the AD server login credentials to:

- Connect to the AD server and create the RAC device objects in the AD server.
- Connect to the AD server and set an association object and a privilege object for each RAC.

You can have multiple association objects, and each association object can be linked to as many users, groups of users, or RAC device objects as required. The users and RAC device objects can be members of any domain in the enterprise. However, each association object can be linked (or, may link users, groups of users, or RAC device objects) to only one privilege object.

For extended schema configuration, depending on the RAC type, the respective extended schema objects must be assigned. For example, the old extended schema objects are assigned to DRAC 4, DRAC 5, and CMC and the new extended schema objects are assigned to iDRAC6 and iDRAC7. For more information on extended schema, see the appropriate RAC user guide listed in Other Documents You May Need.

To create RAC objects and configure RACs using extended schema based AD settings:

1. Discover and verify the RAC IP addresses on your network. For more information, see Discovering Importing and Verifying RACs.
2. In the **Firmware Update Configuration** window, click **Next**.

   The **Active Directory Configuration** window is displayed.
3. Under **Filter on Schema**, select one of the following options to filter the RACs that you want to configure:

   - Standard Schema
   - Extended Schema
   - Active Directory disable

     When you select a filter type, the corresponding RAC IP addresses are selected from the list. You can also select individual RAC IP addresses from the list.
4. Under **New Schema**, select **Extended Schema** and click **Next**.

   The **Common Settings** window is displayed. The settings provided in this window are common for both standard and extended schema.
5. Enter the following:

   - Under **Upload Active Directory CA certificate**, click **Browse** and select the CA certificate file to be uploaded.

NOTE: This is optional for iDRAC6 and iDRAC7, but mandatory for DRAC 4, DRAC 5, and CMC. The AD CA certificate on the RAC must be the same certificate that is on the AD server. For iDRAC6 and iDRAC7, if the certificate is not specified, the default SSL certificate is used.

   - If you have selected the IP addresses for iDRAC6 or iDRAC7, click the **iDRAC6/iDRAC7** tab and enter the AD settings. For information about the settings, see *Dell Remote Access Configuration Tool Online Help*.
   - If you have selected IP addresses for DRAC4, DRAC5, or CMC, click the **DRAC4 / DRAC5 / CMC** tab and enter the AD settings. For information about the settings, see *Dell Remote Access Configuration Tool Online Help*.

6. Click **Next**.

   The **Extended Schema Settings** window is displayed.

7. Create RAC device object names that must be configured on the AD server; the AD RAC objects uniquely identifies the RACs in the AD server. You can do this in one of the following ways:

   - Select the RAC IP addresses, enter the information in the fields, and click **Create Names** to create the AD RAC device object names in the **Name** column. For information about the settings, see *Dell Remote Access Configuration Tool Online Help*.
   - Enter the RAC device object name in the **Name** column.

8. Click **Next**.

   The **Active Directory Server Configuration for Extended Schema** window is displayed.

9. Enter the following information:

   - **Network Address** - Enter the IP address of the AD server.
   - **User Name** - Enter the user name to login to the AD server.
   - **Password** - Enter the password to login to the AD server.

10. Set an association and privilege object for each RAC type. To do this, click the tab for your RAC type, and set the following:

    - Association object - For information on the steps, see Setting an Association Object.
    - Privilege object - For information on the steps, see Setting a Privilege Object.

11. Click **Update Directory** to create RAC device objects on the AD server. If the RAC device objects are created successfully, the status in the **Status** column displays **Updated in Active Directory** for each IP address. If not, the **Status** column displays **Failed to Update Active Directory**.

12. Click **Apply**.

    The **Summary** window displays the following information:

    - Selected RAC IP addresses
    - DNS name
    - RAC type
    - Firmware version
    - Status information
    - Status bar.

      If the configuration is successful, the **Status** column displays the following messages in a sequence for each IP address:

      * Uploading CA certificate - This message is displayed only if you have enabled CA certificate validation.
      * Configuring - RAC configuration is in-progress.
      * Configuration Success - RAC configuration is successful.

If the configuration is not complete, the **Status** column displays one of the following messages for the IP address(es):

- * Certificate Upload Failed - CA certificate uploaded is invalid.
- * Configuration Failed - RAC configuration is not successful.
- * Insufficient Privileges - The required privileges are not provided to configure the RAC.

For more information on the **Status** column messages, see Troubleshooting and Frequently Asked Questions.

After all the configurations are completed, the message "Done" is displayed.

13. Click **OK** and then click **Finish** to close the application.

Setting an Association Object

An association object provides the connection between the users with specific privileges and the devices. To set an association object:

1. In the **Active Directory Server Configuration for Extended Schema** window, click **Browse Directory** for the **Association Object** field.

   The **Browse for Dell iDRAC Association Object** dialog box is displayed.
2. Navigate and double-click **Dell** to display the available objects.

   The displayed association, privilege, and device object icons are:

   – — Association object for iDRAC6 and iDRAC7.

   – — Association object for DRAC 4, DRAC 5, and CMC.

   – — Privilege object for all schema.

   – — Device object for DRAC 4, DRAC 5, and CMC.

   – — Device object for iDRAC6 and iDRAC7.
3. Select the association object based on the RAC type and click **Select**.

   The selected association object is displayed as a string in the **Association Object** field.

Setting a Privilege Object

A privilege object defines the user's or group's privileges when authenticating to a RAC device. A privilege object must be in the same domain as the association object.

To set a privilege object:

1. In the **Active Directory Server Configuration for Extended Schema** window, click **Browse Directory** for the **Privilege Object** field.

   The **Browse for Dell Privilege Object** dialog box is displayed.
2. Navigate and double-click **Dell** to display the available objects.

   The displayed association, privilege, and device object icons are:

   – — Association object for iDRAC6 and iDRAC7.

   – — Association object for DRAC 4, DRAC 5, and CMC.

   – — Privilege object for all schema.

   – — Device object for DRAC 4, DRAC 5, and CMC.

   – — Device object for iDRAC6 and iDRAC7.

3. Select the privilege object related to the association object that you had specified and click **Select**.

   The selected privilege object is displayed as a string in the **Privilege Object** field.

Disabling AD Standard or Extended Schema for RACs

You can disable the AD standard or extended schema configuration for a selection of the discovered and verified RACs on your network. To disable AD standard or extended schema for RACs:

1. Discover and verify the RAC IP addresses on your network. For information on the steps, see Discovering Importing and Verifying RACs.
2. In the **Firmware Update Configuration** window, click **Next**.

   The **Active Directory Configuration** window is displayed.
3. Filter the RACs that are configured to a standard or extended schema and disable AD schema for the filtered RACs. To do this, under **Filter on Schema**, select one of the following options to filter the RACs that you want to configure:

   – Standard Schema
   – Extended Schema
   – Active Directory disable

     When you select a filter type, the corresponding RAC IP addresses are selected from the list. You can also select individual RAC IP addresses from the list.
4. Under **New Schema**, select **Disable Active Directory** and click **Apply**.

   If the configuration is successful, the **Status** column displays the following messages in a sequence for each IP address:

   – Configuring - RAC configuration is in-progress.
   – Configuration Success - RAC configuration is successful.

   If the configuration is not completed, the **Status** column displays one of the following messages for the IP address:

   – Configuration Failed - RAC configuration is not successful.
   – Insufficient Privileges - The required privileges are not provided to configure the RAC.

     For more information on the **Status** column messages, see Troubleshooting and Frequently Asked Questions.

   After all the configurations are completed, the message "Done" is displayed.
5. Click **OK**.

   The AD standard or extended schema configuration is disabled for the selected RACs.

6

Troubleshooting and Frequently Asked Questions

1. **DRACT does not discover a RAC.**

   Make sure that you have performed the following:

   – Ping the RAC IP address to make sure that you can connect to the RAC from your host.
   – The HTTP protocol is not blocked on the host system. Check your network proxy settings and make sure that the proxy is configured correctly to allow connectivity to the Internet.
   – The RAC has the remote RACADM feature enabled.

2. **DRACT only discovers DRAC4 controllers.**

   Make sure that the HTTP protocol is not blocked on the host system. Check your network proxy settings and make sure that the proxy is configured correctly to allow connectivity to the Internet.

3. **RAC verification fails with the message Verification Failed.**

   The discovered RAC may be unsupported. Sometimes, a DRAC 3, DRAC/MC, or ERA/MC controllers may be discovered as a DRAC 4 controller. Make sure that the controller is not an unsupported controller. For a list of supported RACs, see Supported RACs.

   The RAC firmware may be in an undefined state. Before performing RAC verification, login to the RAC using remote RACADM or the Web GUI to make sure that the RAC is working correctly.

4. **RAC verification fails with the message Access Denied.**

   The user name and the password provided to verify the RAC do not have login privileges or is not a valid account to access the controller.

5. **Firmware update failed with the message Insufficient Privileges.**

   The user name and password provided during RAC verification do not have RAC configuration privileges.

6. **Firmware update failed with the message Failed to initiate.**

   The RAC firmware is in an undefined state or is not accessible remotely. Remove and plug the power cord back on your system and make sure that the RAC is accessible before performing the firmware update using DRACT.

7. **Firmware update fails with the message Firmware update failed.**

   The controller was in an undefined state or there was a known firmware update issue on the particular firmware version. For the solution, see the readme file for the specific firmware version before updating the firmware again.

8. **Firmware update failed with the message Unable to find firmware image.**

   The firmware image is not available in the specified TFTP server path. Make sure that the image is available in this path.

9. **AD update fails with the message Failed to Update Active Directory.**

   Make sure that you have followed the AD setup steps documented in the appropriate RAC user guide to set up the AD server and to enable AD authentication to the RAC.

   Make sure that you provide the AD credentials that have configuration privilege on the domain controller.

10. **Standard schema or extended schema failed with the message Certificate Upload Failed.**

    The CA certificate uploaded is invalid. Check and upload the valid CA certificate. For more information, see the respective RAC user's guide.

11. **Standard schema, extended schema, or AD schema disabled failed with the message Insufficient Privileges.**

The user name and password provided to verify the RAC IP addresses do not have configuration privileges on the RAC.

12. **Standard schema, extended schema, or AD schema disabled fail with the message Configuration Failed.**

    The RAC was in an undefined state or there was a known configuration update issue on a particular firmware version. For the solution, see the readme file for the specific firmware version before updating the firmware again.