



Device Management Using ACS

Table of Contents

- Preface..... 1
- CVD Navigator 2
 - Use Cases 2
 - Scope 2
 - Pro ciency..... 2
- Introduction 3
 - Techno(U)2.1(se)-5(C)-0.7(a)0.5(se)T0 Tc -0.921 Tw /Span/ActualTextFEFF002E>>> BDC -9.612 0



Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or



CVD Navigator

Introduction

Technology Use Case



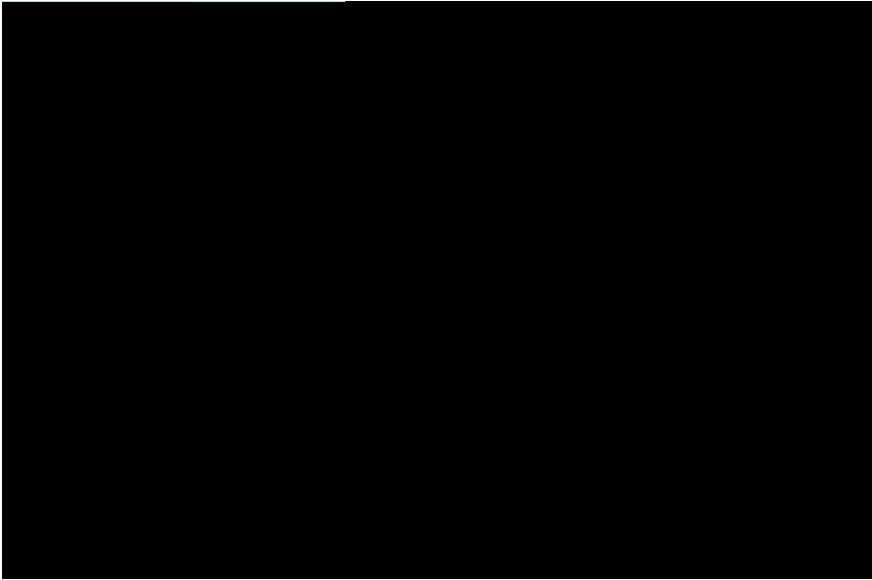


Procedure 6 Create an external identity store

An *external identity store* allows designated users to authenticate against a network device by using their pre-existing credentials. You can also use attributes (such as group membership) in the external store when defining

Step 4:

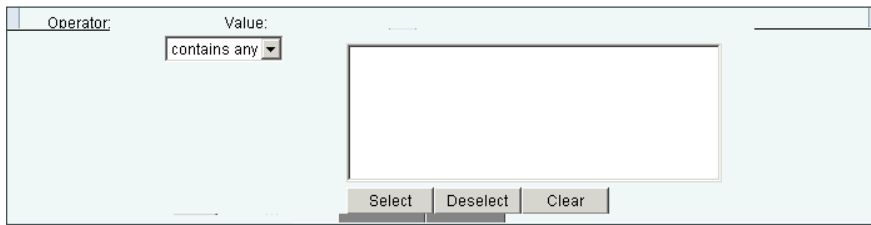
Step 6: Click Save Changes.



Step 6: Select Group Mapping

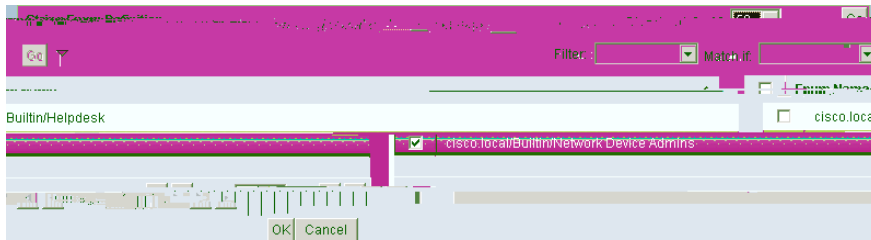


Step 15: Under Value, click **Select**.



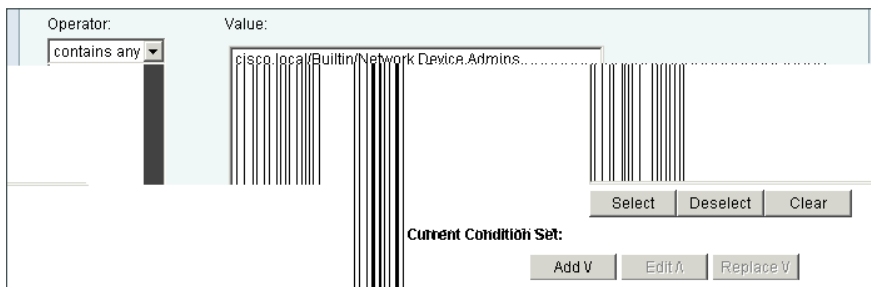
The screenshot shows a configuration window with two main sections: 'Operator' and 'Value'. The 'Operator' dropdown is set to 'contains any'. The 'Value' field contains a large, empty rectangular text box. Below the text box are three buttons: 'Select', 'Deselect', and 'Clear'.

Step 16: Choose a Microsoft Active Directory group, and then click **OK**.



The screenshot shows a search dialog box with a search bar at the top. Below the search bar is a list of search results. The first result, 'cisco.local/Builtin/Network Device Admins', is selected with a checkmark. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Step 17: Click **Add V**.



The screenshot shows the configuration window with the 'Value' field now populated with the text 'cisco.local/Builtin/Network Device Admins...'. Below the 'Value' field is a section titled 'Current Condition Set:' with three buttons: 'Add V', 'Edit V', and 'Replace V'. The 'Select', 'Deselect', and 'Clear' buttons from the previous step are still visible above the 'Current Condition Set' section.

Step 18: To the right of Identity Group, click **Select**. This is the identity group to which the Microsoft Active

Step 2: Click Create.

Step 3:

Step 10: Click **Submit**.

Step 11: Repeat this procedure for every security device that you want to limit access to.

Procedure 3 Exclude users from Security Devices group

This procedure edits the existing authorization rule to prohibit Helpdesk users from logging in to security devices.

Step 1: Navigate to **Access Policies > Access Services > Default Device Admin > Authorization**.

Step 9: Click Save Changes.

