This section describes how to configure role-based access control (RBAC) on the Cisco 4700 Series Application Control Engine (ACE) appliance.

Guide Contents
Overview
Setting Up an ACE Appliance
Creating a Virtual Context
Configuring Access Control Lists
Configuring Role-Based Access Control (this section)
Configuring Server Load Balancing
Configuring a Load-Balancing Predictor
Configuring Server Persistence Using Stickiness
Configuring SSL Security
Configuring Health Monitoring Using Health Probes

Contents

Overview

After reading this section, you should have a basic understanding of how the ACE appliance provides security administration by using RBAC and how to configure a server maintenance user with permission to access a subset of your network.

One of the most challenging problems in managing large networks is the complexity of security administration. The ACE appliance allows you to determine the commands and resources available to each user through RBAC. In RBAC, users are associated with domains and roles.

A domain is a collection of physical and virtual network resources such as real servers and virtual servers.

User roles determine a user's privileges, such as the commands that the user can enter and the actions the user

can perform in a particular context. The ACE provides a number of predefined roles. In addition, administrators in any context can define new roles.

The ACE provides the following predefined roles, which you cannot delete or modify:

- Admin?If created in the Admin context, has complete access to, and control over, all contexts, domains, roles, users, resources, and objects in the entire ACE. If created in a user context, gives a user complete access to and control over all policies, roles, domains, server farms, real servers, and other objects in that context.
- Network Admin?Has complete access to and control over the following features:
  - Interfaces
  - Routing
  - Connection parameters
  - Network Address Translation (NAT)
  - VIPs
  - Copy configurations
  - changeto **command**
- Network-Monitor?Has access to all **show** commands and to the **changeto** command. If you do not explicitly assign a role to a user with the **username** command, this is the default role.
- Security-Admin?Has complete access to and control over the following security-related features within a context:
  - ACLs
  - Application inspection
  - Connection parameters
  - Interfaces
  - Authentication, authorization, and accounting (AAA)
  - NAT
  - Copy configurations
  - **changeto** command
- Server-Appln-Maintenance?Has complete access to and control over the following features:
  - Real servers
  - Server farms

- Load balancing
- Copy configurations
- **changeto** command

- Server-Maintenance?Can perform real server maintenance, monitoring, and debugging for the following features:
  - Real servers?Modify permission
  - Server farms?Debug permission
  - VIPs?Debug permission
  - Probes?Debug permission
  - Load balancing?Debug permission
  - **changeto** command?Create permission
- SLB-Admin?Has complete access to and control over the following ACE features within a context:
  - Real servers
  - Server farms
  - VIPs
  - Probes
  - Load balancing (Layer 3/4 and Layer 7)
  - NAT
  - Interfaces
  - Copy configurations
  - **changeto** command
- SSL-Admin?Can administer all SSL features:
  - SSL?Create permission
  - PKI?Create permission
  - Interfaces?Modify permission
  - Copy configurations?Create permission
  - **changeto** command?Create permission

You can create a user and assign them privileges through RBAC as follows:

1. Create a domain and choose network resources for the domain.

2. Create a user and associate the user with the following:

    ◊ A role (predefined or custom)

    ◊ A domain

This section describes how to create a domain and a user, and how to associate the user with a predefined role and the new domain. For more information on predefined roles and how to define a custom role, see Cisco ACE 4700 Series Appliance Virtualization Configuration Guide.

To create a domain and a user, you can use either the ACE Device Manager GUI or the CLI.

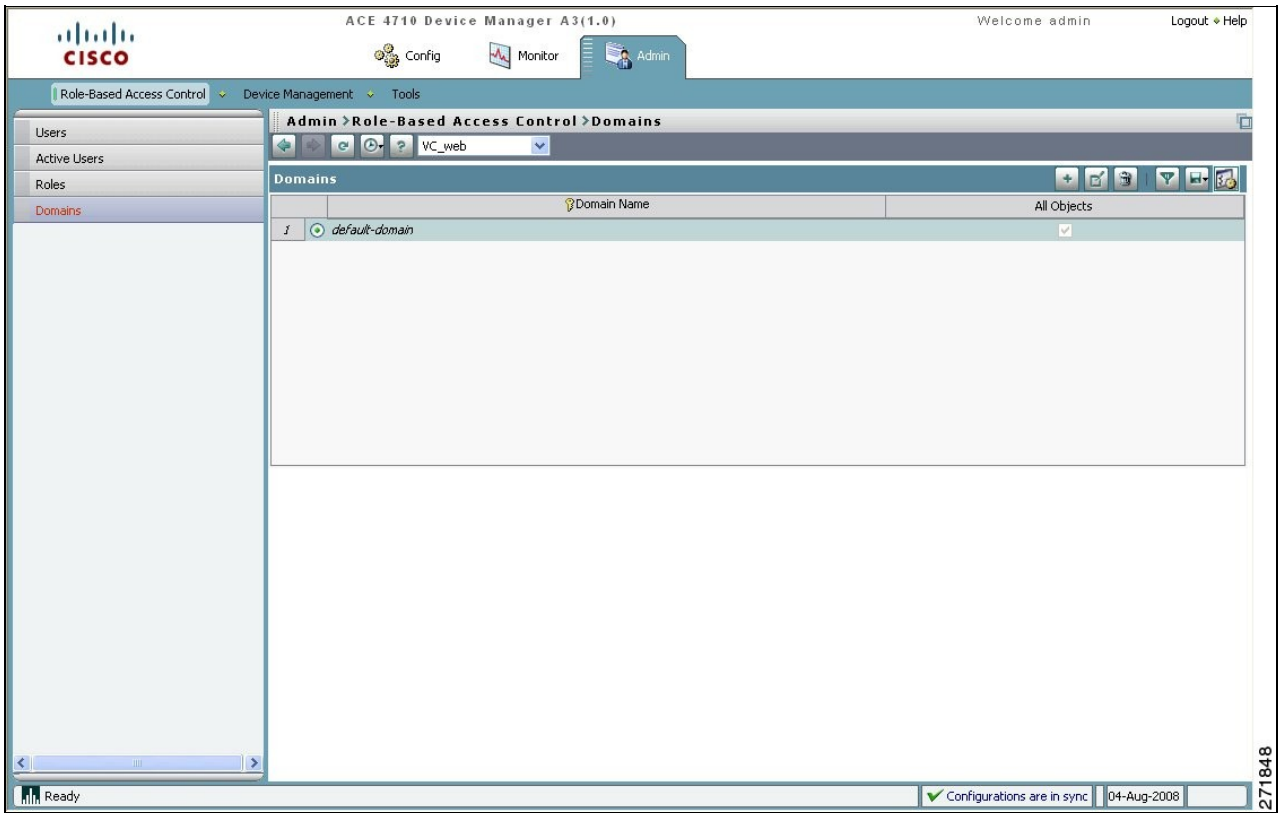
Configuring RBAC Using the Device Manager GUI

In this procedure, you use the GUI to create a domain that includes the user context that you created in Creating a Virtual Context and then create a server maintenance user, user1, to manage those servers. Configure this RBAC setup using the GUI by following these steps:

1. Choose **VC_web**.

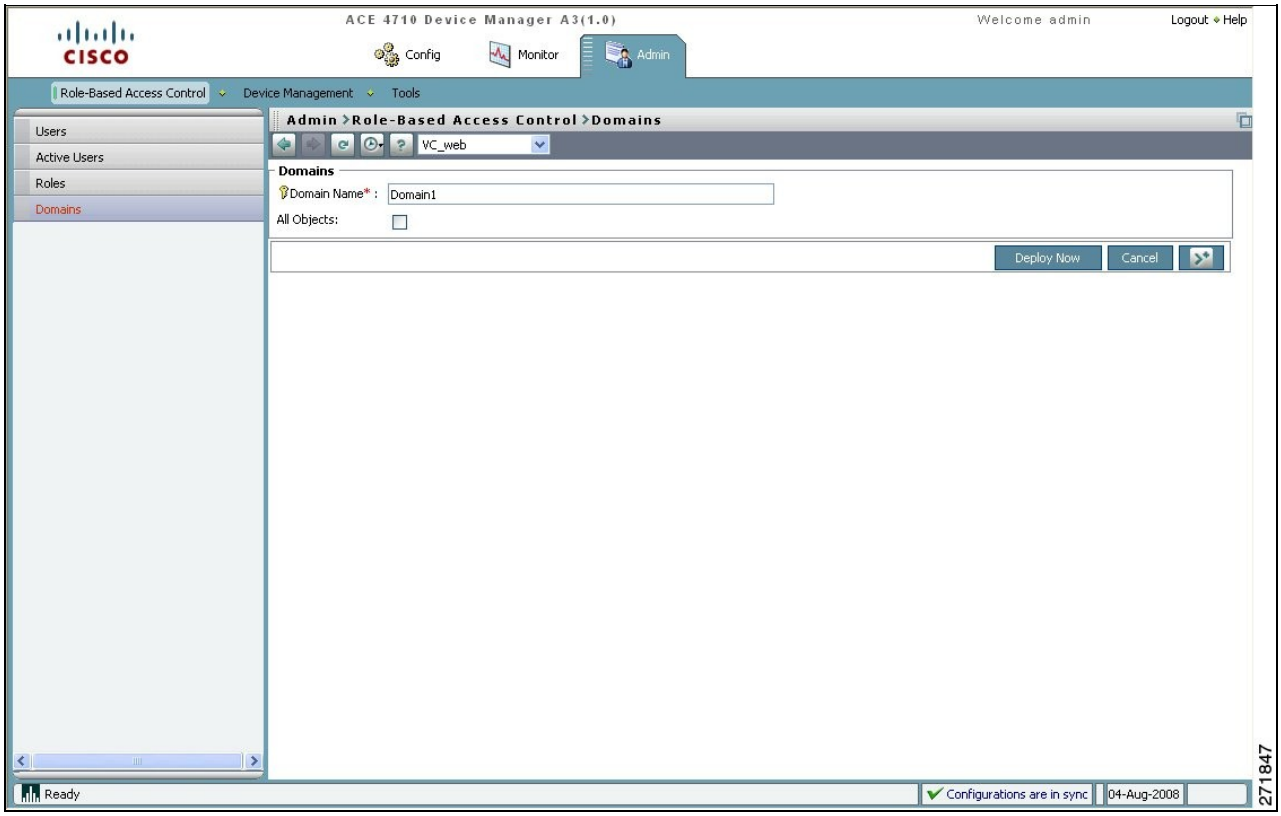
2. Choose **Admin > Role-Based Access Control > Domains**. The Domains pane appears (Figure 1).

Figure 1 Domains Pane



3. Click **Add** to add a new domain. The New Domain window appears (Figure 2).

Figure 2 Domains Window



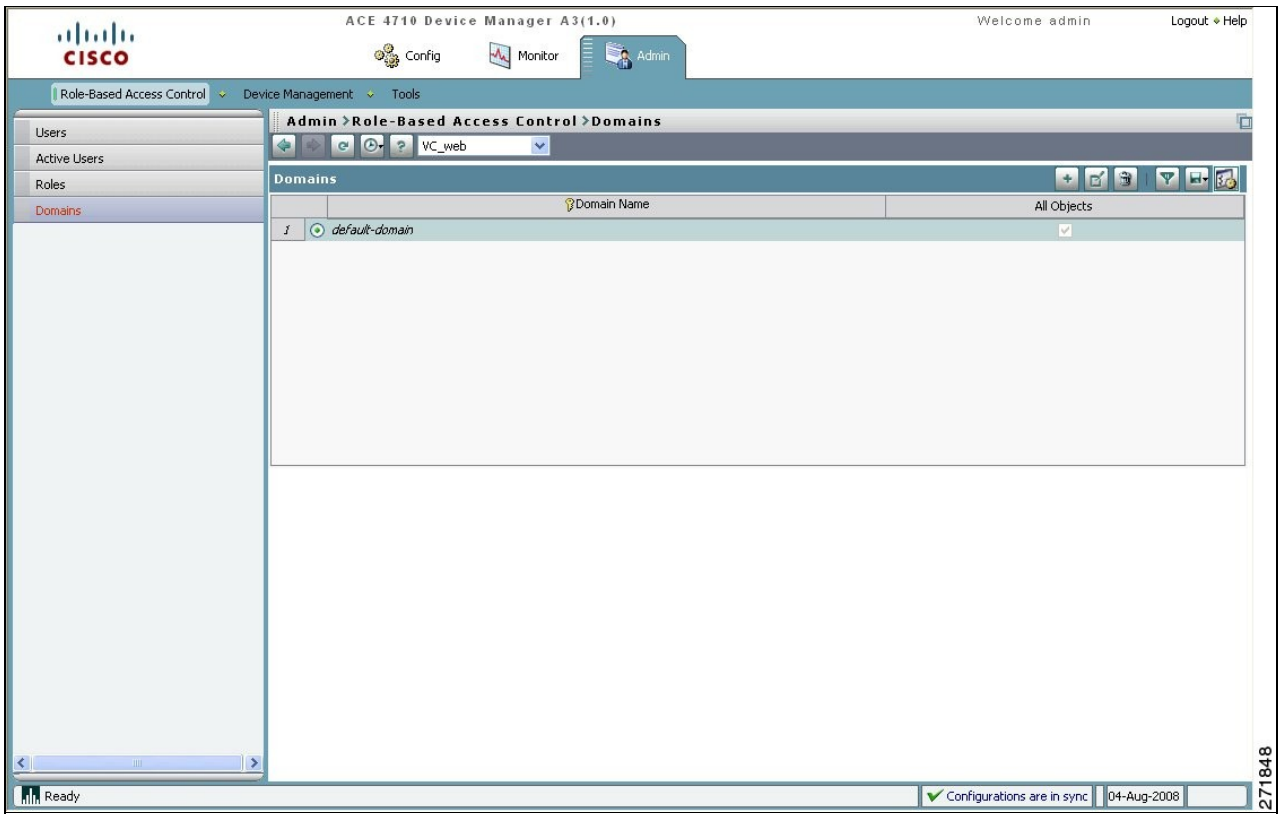
4. Enter **Domain1** for the Domain Name.

5. Select **All Objects**.

6. Click **Deploy Now** to create a domain that includes all objects in context VC_web.

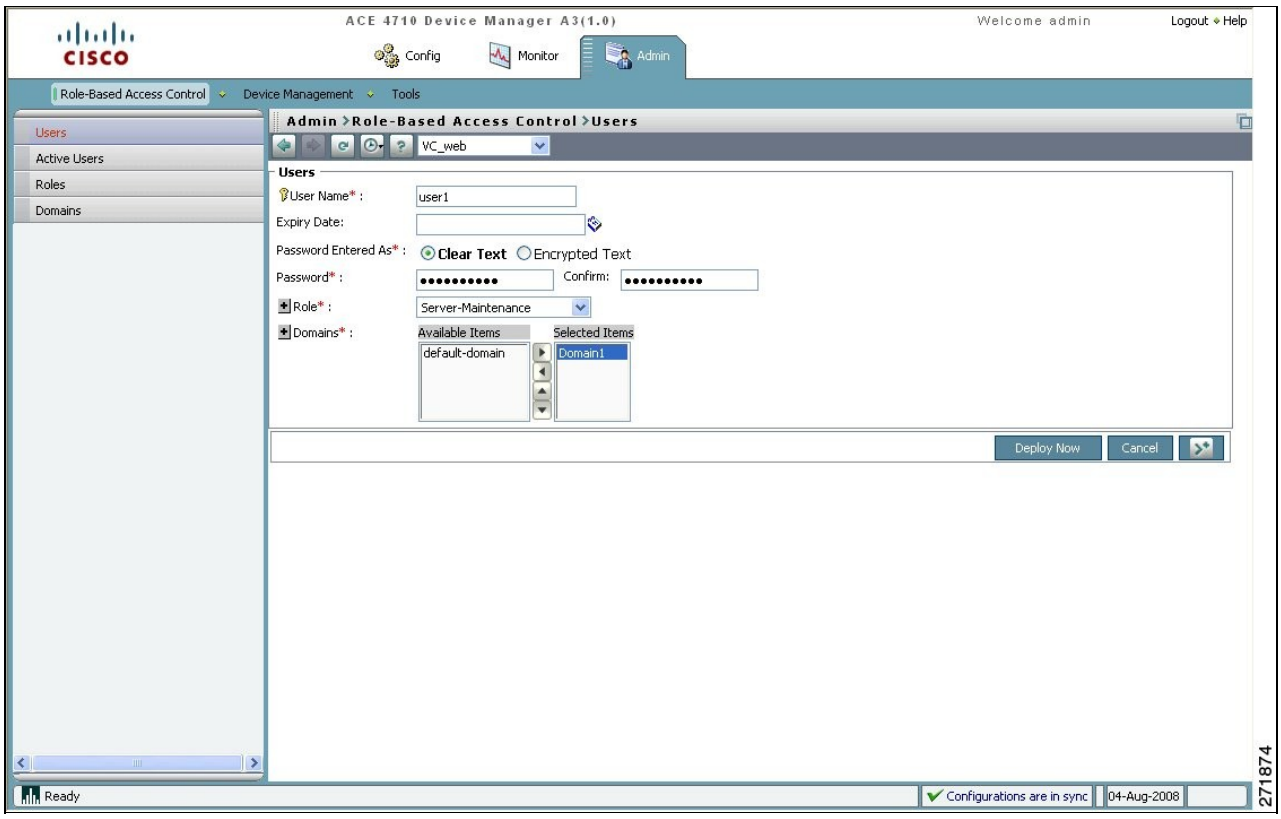
7. Choose **Role-Based Access Control > Users** to create a user. The Users pane appears (Figure 3).

Figure 3 Users Pane



8. Click **Add**. The User window appears (Figure 4).

Figure 4 Users Window



9. Enter the following user attributes. Leave the remaining attributes blank or with the default values.

   ◊ User Name: user1

   ◊ Password: MYPASSWORD

   ◊ Confirm: MYPASSWORD

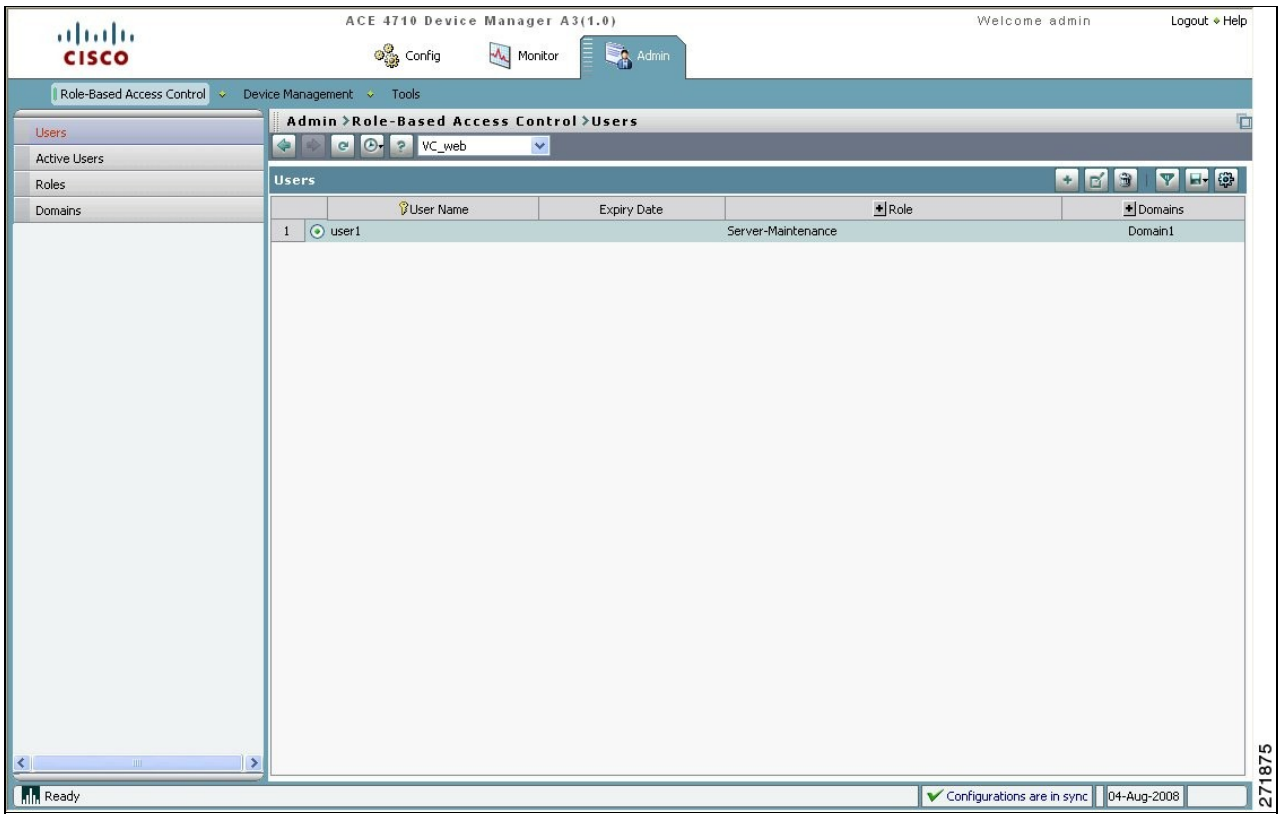
   ◊ Role: Server-Maintenance

10. Choose **Domain1** and click the **right-arrow** button. Domain1 is moved to the Selected Items list.

11. Choose **default-domain** and click the **left-arrow** button. Default-domain is removed from the Selected Items list.

12. Associate the new user user1 with the role Server-Maintenance and the domain Domain1 by clicking **Deploy Now**. The new user is added to the Users pane (Figure 5).

Figure 5 Users Pane with user1 Added



Configuring RBAC Using the CLI

Configure RBAC using the CLI by following these steps:

1. Verify that you are operating in the desired context by checking the CLI prompt. If necessary, change to the correct context.

```
host1/Admin# changeto VC_web

host1/VC_web#
```

2. Enter configuration mode.

```
host1/VC_web# Config

host1/VC_web(config)#
```

3. Create a domain for the context.

```
host1/VC_web(config)# domain Domain1

host1/VC_web(config-domain)#
```

4. Allocate all objects in the VC_web context to the domain.

```
host1/VC_web(config-domain)# add-object all

host1/VC_web(config-domain)# exit

host1/VC_web(config)#
```

5. Configure new user user1, and assign the predefined role TECHNICIAN and the domain Domain1 to the user.

```
host1/VC_web(config)# username user1 password 5 MYPASSWORD role TECHNICIAN domain Domain1
```

Note The parameter 5 for password is for an MD5-hashed strong encryption password. Use 0 for a clear text password.

```
host1/VC_web(config)# exit
```

6. Display the user and domain configurations.

```
host1/VC_web# show running-config role

host1/VC_web# show running-config domain
```

In this section, you have created a user to perform a limited number of functions on a subset of your network. Next, you will create a virtual server for server load balancing.