CloudAccess

Installation and Configuration Guide

October 2017

Legal Notice

About this Book and the Library

The *Installation and Configuration Guide* provides conceptual information about the NetIQ CloudAccess (CloudAccess) product. This book contains configuration information for the appliance and for the SaaS applications.

Intended Audience

This book provides information for individuals responsible for deploying and configuring the appliance, managing identity sources, and configuring application connectors.

Other Information in the Library

The library provides the following information resources:

Connectors Guide

Provides conceptual and procedural information for configuring and managing application connectors.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for fields in windows of the administration console.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

Contents

About this Book and the Library 3
About NetIQ Corporation 5

1 Overview of CloudAccess 11

The Problem of Securing Resources 11
The Solution That CloudAccess Provides. 13
How CloudAccess Works 14

2 Installing the Appliance 17

Installation and Configuration Checklist 17
Product Requirements 18
Appliance Installation Worksheet 21
Deploying the Appliance 22
Upgrading Your Environment 23
Initializing the Appliance 23
Changing Initialization Settings. 24

3 Configuring the Appliance 25

Getting Started 25
Registering the Appliance 26
Configuring Identity Sources. 26
Configuring Networking Options and Certificates 27
- Configuring the Forward Proxy 27
- Configuring the Second Network Interface 27
- A Sample Network Configuration 28
- Configuring the Routing Table 29
- Changing the Certificates on the Appliance 29

Configuring Clustering 30
- Advantages of Clustering. 30
- Adding Nodes to the Cluster 30
- Promoting a Node to Master 31
- Removing a Node from the Cluster 32
- Configuring an L4 Switch for Clustering. 32

Configuring an L4 Switch for Email Proxy. 33
- Configuring the SMTP Protocol Handler 33
- Configuring the POP Protocol Handler. 34
- Configuring the IMAP Protocol Handler 34

4 Configuring LDAP and JDBC Identity Sources 37

Understanding LDAP Identity Sources 37
- Active Directory Requirements. 37
- eDirectory Requirements 38
- Understanding LDAP Advanced Options 39

Understanding JDBC Identity Sources 40
- JDBC Requirements 40
- Obtaining the Script Files. 41

Populating the Required Columns . . . 41
Dataflow Information . . . 42
Configuring an LDAP or JDBC Identity Source . . . 45

5 Configuring Social Identity Sources 49

Understanding Social Media Identity Sources in CloudAccess. . . . 49
Understanding Linked Logins in CloudAccess . . . 49
Configuring the Connector for Linked Logins . . . 50
Configuring Active Directory as an Identity Source . . . 50
Configuring eDirectory as an Identity Source . . . 51
Configuring reCAPTCHA for Active Directory or eDirectory . . . 52
Configuring Facebook as an Identity Source . . . 52
Configuring Google as an Identity Source . . . 53
Configuring LinkedIn as an Identity Source . . . 53
Configuring MSLive as an Identity Source . . . 54
Configuring Twitter as an Identity Source . . . 55
Configuring Yahoo as an Identity Source . . . 55
Configuring OAuth2 Sites as Identity Sources . . . 56
Configuring OpenID Connect Sites as Identity Sources . . . 57

6 Configuring Self-Service Registration and Password Management 59

Enabling a Self-Service User Store . . . 59
Using SSUS as an Authentication Source for an Application . . . 60
Granting SSUS Users Access to a Private Application . . . 60
Denying SSUS Users Access to an Application . . . 61
Using the Self-Service User Registration and Password Management Services . . . 61
Providing Help Desk Services for Self-Registered Users . . . 62
Assigning a User to the Help Desk Role . . . 62
Resetting the Password for a Locked Self-Registered User Account . . . 62
Deleting a Self-Registered User Account . . . 63

7 Configuring SAML 2.0 Inbound Identity Sources 65

8 Configuring Roles Management 67

Understanding CloudAccess Role Types . . . 67
Assigning Roles to Users . . . 68

9 Configuring Authentication Methods 69

Configuring Integrated Windows Authentication with Kerberos . . . 69
Configuring the Kerberos User in Active Directory . . . 69
Configuring the Appliance to Use Integrated Windows Authentication with Kerberos . . . 70
Configuring User Browsers . . . 70
Configuring Google reCAPTCHA . . . 70
Requirements for reCAPTCHA . . . 71
Configuring Intrusion Detection for Failed Logins . . . 71
Configuring a Google reCAPTCHA Account . . . 72
Configuring the reCAPTCHA Tool . . . 73
Configuring the TOTP Tool for Two-Factor Authentication Using Google Authenticator . . . 74
Configuring the TOTP Tool . . . 74
Registering a Mobile Device with the TOTP Tool for OTP Generation . . . 75
Using Two-Factor Authentication at Login . . . 77

Resetting a Device (Unregistering a Device) 77
Configuring the Advanced Authentication Tool for Two-Factor Authentication Using the Advanced Authentication Appliance. 78
Requirements for Advanced Authentication 79
Configuring the Advanced Authentication Tool 79
Configuring FIDO for Two-Factor Authentication 80
Requirements for FIDO 80
Configuring the FIDO Tool 80
Resetting (Unregistering) a FIDO Device. 81

10 Configuring Mobile Access for Users 83

Introduction to Mobile Access 83
Configuring the Mobile Tool on the Appliance. 83
Replacing the Default Certificate on the Appliance. 84
Generating a Self-Signed Certificate 84
Installing a Self-Signed Certificate on the Mobile Device. 85
Helping Users Register Their Mobile Devices. 86
Registering iOS Devices 86
Registering Android Devices 86
Understanding the MobileAccess PIN 87
Unregistering Mobile Devices 88

11 Configuring Connectors 89

12 Mapping Authorizations 91

Supported Roles and Authorizations. 91
Prerequisites. 92
Loading Authorizations 92
Reloading Authorizations 92
Mapping Authorizations. 93
Understanding Google Apps Mappings 94
A Mapping Example 94
Approving Requests 95

13 Reporting 97

Using Google Analytics as an External Dashboard 97
Integrating with Sentinel Log Manager 97
Configuring CloudAccess to Forward Events to a Syslog Server 98

14 Configuring the End User Experience 99

Configuring Email Clients 99
Enabling Google Mail Proxy 99
Configuring End User Browsers for Kerberos Authentication 100
Customizing Branding on User-Facing Pages 101
Configuring User Session Timeouts 102

15 Maintenance Tasks 103

Changing the Cluster Password 103
Changing the IP Address 103
Changing the Public DNS Name or NTP Server Settings, or Uploading New Certificates 103

Updating the Appliance . . . 104
Shutting Down or Rebooting a Node . . . 105
Recovering from a Disaster . . . 105

16 Troubleshooting CloudAccess 107

Troubleshooting the Appliance Initialization . . . 107
Displaying Health . . . 107
Using Troubleshooting Tools . . . 107
Troubleshooting Different States . . . 109
Master Node Health . . . 109
Front Panel of the Node . . . 109
Top of the Node . . . 110
Identity Source . . . 111
Applications . . . 112
Tools . . . 112
Understanding Support for International Characters . . . 113
Troubleshooting Provisioning Issues . . . 114
Capturing Logs for Provisioning Issues . . . 114
Understanding the Result of Actions Performed on Users and Groups . . . 114
Users No Longer See Private Appmarks . . . 115
Active Directory LDAP Search Treats Extended Characters and Normal Characters the Same . . . 116
Non-Alphanumeric Characters in the Group Description Result in Users Seeing No Appmarks . . . 116
Cannot Change User or Group Filter and Change Naming Attribute in Same Operation . . . 116
Troubleshooting Policy Mapping Issues . . . 116
No Connectors Appear on the Policy Mapping Page . . . 116
CloudAccess Does Not Reconcile Pending Approvals with Changes to Policy Mappings . . . 117
Using Multiple Browsers or Browser Windows Can Result in Duplicate Mappings . . . 117
Troubleshooting Mobile Device Issues . . . 117
Safari on Mobile Devices Cannot Access the Login Page After You Enable the Mobile Tool. . . 117
Device Registration Issues. . . 117
Troubleshooting CloudAccess Login Failures . . . 117
Users See a General Login Error . . . 118
Troubleshooting Authentications or Single Sign-On Issues . . . 118
Troubleshooting Connector Issues . . . 118
Troubleshooting JDBC Identity Source Issues . . . 118

A Performing Advanced Branding 121

//Shared Include Files . . . 121
//Standard Login Page . . . 122
//Second Factor Authentication Login Pages . . . 122
//Landing Page (Home Page after Login) . . . 122
//Logout Page . . . 122

1 Overview of CloudAccess

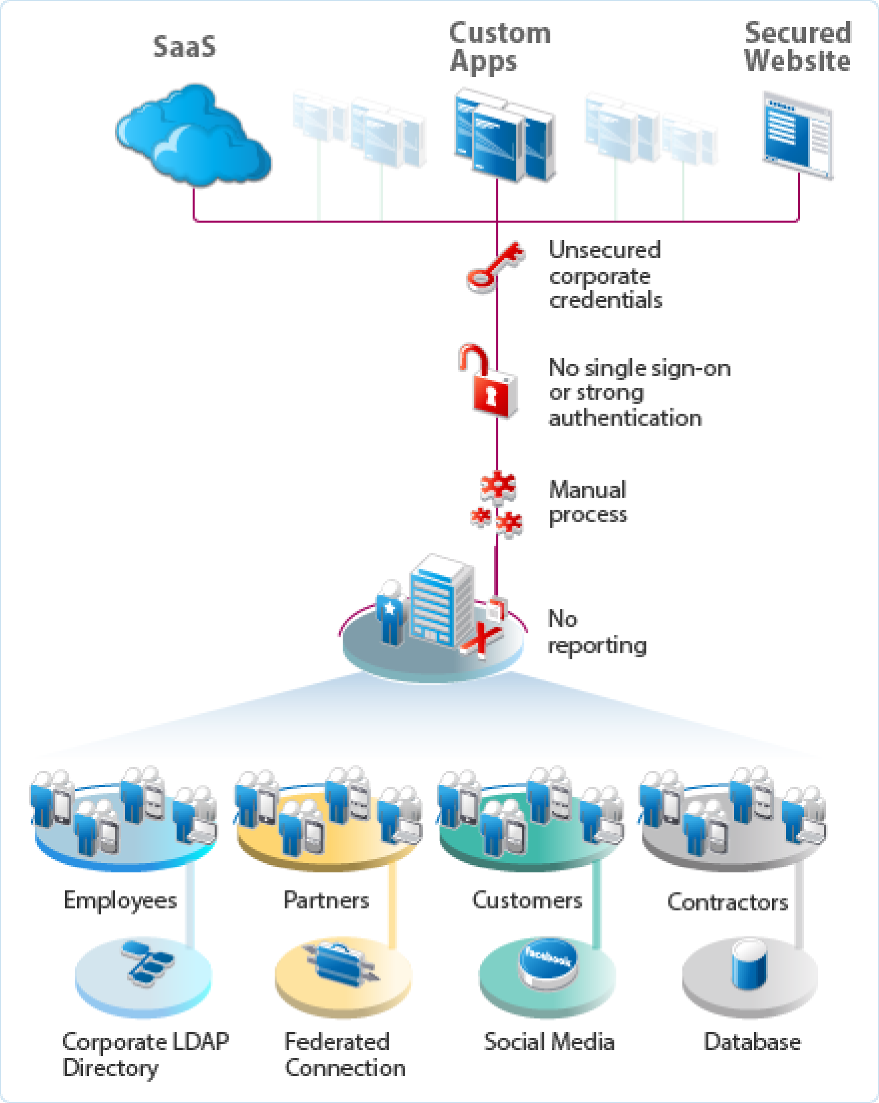
CloudAccess is a virtual appliance that enables you to provide secure access to resources that your organization controls for many different types of users.

The Problem of Securing Resources

As a corporation, government office, educational institution, or other type of organization, you might have many different types of users who want access to resources you control. Some of those resources might be internal and some might be Software as a Service (SaaS) applications.

This situation presents many different complex problems for your organization. The following image depicts some of the problems you might face.

Figure 1-1 Problems Securing Resources



Common problems include the following:

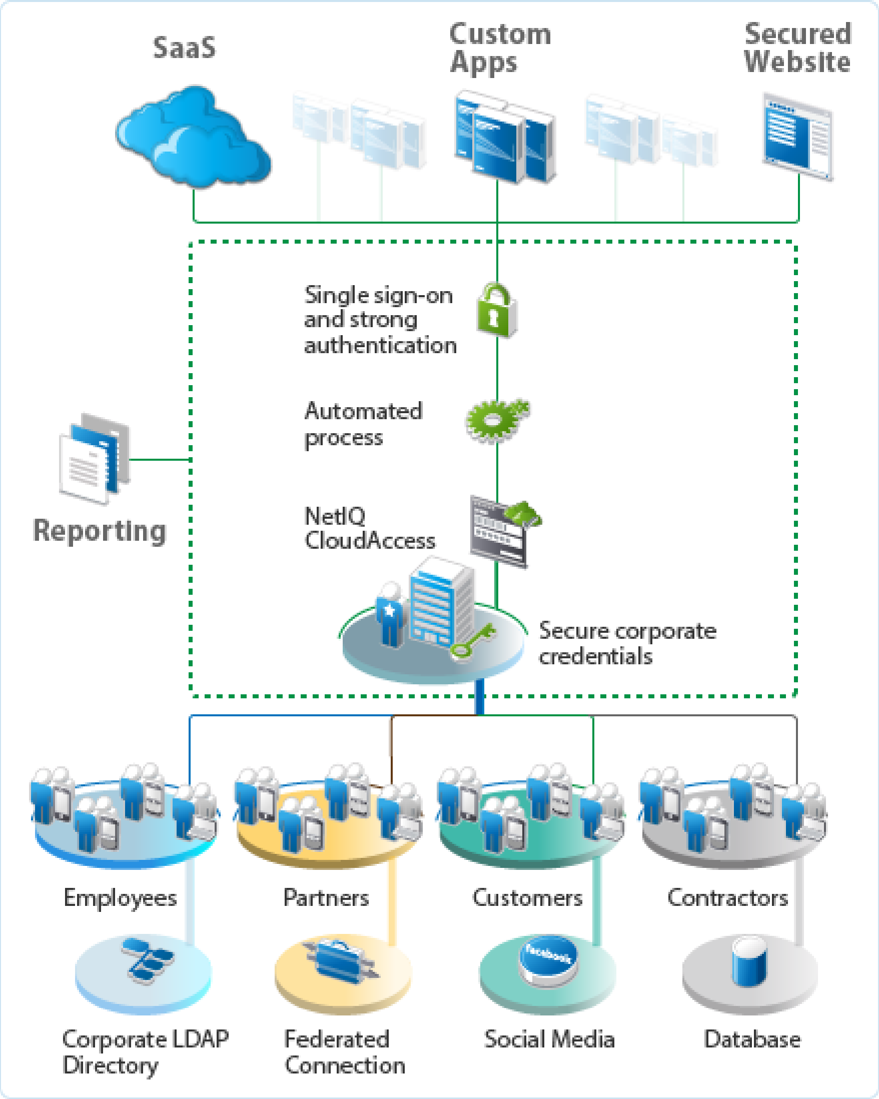
- Different types of users request access to resources you control.
- Different types of users require different access levels to resources. For example, your customers would like to use an existing social media account to access your rewards program instead of having to create a new account.
- Users must wait for the IT department to create accounts in the SaaS applications. It is a manual process whether the IT department creates the account or the user creates the account.
- Users bypass the IT department and create their own accounts in the SaaS applications.
- Users must remember separate passwords for each application, and often use their corporate credentials.
- Administrators receive no compliance reports of user activity in the SaaS applications.

The Solution That CloudAccess Provides

CloudAccess provides a simple, easy-to-deploy appliance that offers a means of providing secure access to resources using a single sign-on account for your users. In addition, CloudAccess enables customers to use their existing social media accounts to access specific applications, such as a rewards program. Users who have both social media accounts and an account in an internal LDAP identity source can link their accounts, which enables them to access all assigned resources using either account.

The following graphic shows how CloudAccess solves the complex problems you face in securing resources for your organization.

Figure 1-2 *CloudAccess Solution*



CloudAccess provides the following benefits:

- The ability to manage many different types of users from many different sources
- An automated process to provision user accounts to the SaaS applications

- Secure single sign-on to the SaaS applications inside or outside of the organization
- Compliance reporting of the users' activities in the resources you provide

How CloudAccess Works

CloudAccess is a virtual appliance that you deploy to your existing IT infrastructure. Here is how CloudAccess works for you:

- **Identity Sources:** You define different identity sources from which you pull user account information for the appliance to use. CloudAccess allows you to define the following types of identity sources:
  - LDAP directories
  - Database
  - Self-Service users
  - Federated connections using SAML 2.0 Inbound authentications
  - Social media accounts
- **Authentication Methods:** You define different authentication methods for users to use when accessing the secure resources. Some of the methods include:
  - One-time-password using Google Authenticator
  - FIDO
  - Integrated Windows Authentication with Kerberos
  - Google reCAPTCHA
  - Advanced Authentication
- **Connectors:** You configure connectors for the applications and resources you want to secure. Some of the connectors automatically provision user accounts from the identity sources to the connected systems, and some of the connectors simply allow for a secure connection.
- **Provisioning:** CloudAccess allows you to map roles (groups) in an identity source, such as Active Directory or eDirectory, to account authorizations in the SaaS applications. CloudAccess leverages group management in the identity source to automatically create and manage the associated user accounts in the SaaS application.

  NOTE: CloudAccess cannot provision users from any social media accounts, or from SAML 2.0 Inbound authentications. These are not full users in CloudAccess and cannot be provisioned.
- **Customers Using Same Account:** CloudAccess also gives you the ability to allow users to use their existing social media accounts to gain access to resources such as a rewards program. These users are different from your corporate users and CloudAccess cannot provision these users.
- **Secure Single Sign-on:** CloudAccess authenticates users against identity sources and provides single sign-on to the SaaS applications and other resources based on the users' entitlements. CloudAccess then authenticates each user to the SaaS application using a user name and a 20-character randomly generated password that is stored only on the appliance.

  The user name and corporate password never leave the appliance. In addition, the user never knows the password to access the resource without going through CloudAccess.
- **Enabling Mobile Devices:** CloudAccess provides an app that enables supported mobile devices to securely access the secured resources.

- **Reporting:** CloudAccess provides reports on the usage of the SaaS applications to help enforce corporate policies and prove compliance.

2 Installing the Appliance

CloudAccess is installed as a virtual appliance using files that you download, extract, and deploy into your IT environment.

Installation and Configuration Checklist

Before you begin installing and configuring your appliance, review the following checklist to ensure that you perform steps in the appropriate order.

Table 2-1 *Installation and Configuration Checklist*

□	Steps	For more information, see...
□	1. Verify that your environment meets all prerequisites.	"Product Requirements" on page 18
□	2. Gather the information you need to install and configure the appliance.	"Appliance Installation Worksheet" on page 21
□	3. Install the appliance.	"Deploying the Appliance" on page 22
□	4. Initialize the appliance.	"Initializing the Appliance" on page 23
□	5. Configure the appliance.	Chapter 3, "Configuring the Appliance," on page 25
□	6. Verify that your identity source meets all requirements, including user attributes, for provisioning users.	◆ "Active Directory Requirements" on page 37 ◆ "eDirectory Requirements" on page 38 ◆ "Understanding JDBC Identity Sources" on page 40
□	7. Configure one or more provisioning identity sources and import users.	Chapter 4, "Configuring LDAP and JDBC Identity Sources," on page 37
□	8. (Optional) Configure social identity sources for external users.	Chapter 5, "Configuring Social Identity Sources," on page 49
□	9. (Optional) Configure additional identity sources as needed.	◆ Chapter 6, "Configuring Self-Service Registration and Password Management," on page 59 ◆ Chapter 7, "Configuring SAML 2.0 Inbound Identity Sources," on page 65
□	10. Configure authentication methods.	Chapter 9, "Configuring Authentication Methods," on page 69
□	11. Configure the Mobile tool on the appliance.	"Configuring the Mobile Tool on the Appliance" on page 83

□	Steps	For more information, see...
□	12. Replace the default certificate on the appliance.	"Replacing the Default Certificate on the Appliance" on page 84
□	13. (Conditional) Install a self-signed or non-public certificate on the mobile device.	"Installing a Self-Signed Certificate on the Mobile Device" on page 85
□	14. Configure the appropriate connectors to enable user access to applications.	"Configuring Connectors" in the *CloudAccess Connectors Guide*
□	15. (Optional) Obtain or create custom icons in `.png` format to represent your appmarked applications.	"Customizing Branding on User-Facing Pages" on page 101
□	16. Configure appmarks for the applications.	"Configuring Appmarks for Connectors" in the *CloudAccess Connectors Guide*
□	17. (Conditional) Map any non-public appmarks to the appropriate groups in the identity source.	"Configuring Appmarks for Connectors" in the *CloudAccess Connectors Guide*
□	18. Map authorizations for users to access the appropriate applications.	Chapter 12, "Mapping Authorizations," on page 91
□	19. (Users) Install the MobileAccess app on their mobile devices and register their mobile devices with the appliance.	"Helping Users Register Their Mobile Devices" on page 86

Product Requirements

Use the information in the following table to verify that your environment meets all requirements before you deploy the appliance.

Table 2-2 *Product Requirements*

Components	Requirements
Supported Virtual Environments	The appliance requires one of the following virtual environments: ◆ Hyper-V on Microsoft Windows Server 2012 R2 ◆ VMware vSphere and vSphere Hypervisor 6.0 ◆ VMware vSphere and vSphere Hypervisor 5.5

Components	Requirements
Virtual System Guest Requirements	Minimum hardware requirements for each appliance node in the cluster: ◆ 60 GB disk space ◆ 2 cores ◆ 8 GB RAM The appliance can be a heavy consumer of CPU, disk I/O, and network bandwidth. Performance can be adversely affected by other virtual machines with similar operational requirements deployed on the same host server. As a best practice, ensure that you group or separate virtual machines on hosts and data stores to avoid resource conflicts for CPU, disk I/O, and network bandwidth. You can do this manually as you deploy virtual machines, or use affinity and anti-affinity rules if they are available in your virtual environment.
Cluster	Supported cluster configuration: ◆ The cluster can have up to five nodes. ◆ For optimal performance, each node should reside in the same IP subnet. **NOTE:** The L4 switch must be configured with the publicly resolvable DNS of the cluster before you initialize the appliance.
Identity Sources	Supported identity sources for provisioning users: ◆ Microsoft Active Directory LDAP on Windows Server 2012 R2 or 2008 R2 ◆ NetIQ eDirectory LDAP 8.8.8 ◆ Microsoft SQL Server 2014 or 2008 ◆ Oracle Database 12c or 11.1 For more information, see Chapter 4, “Configuring LDAP and JDBC Identity Sources,” on page 37. CloudAccess also supports many other types of non-provisioning identity sources, such as social media accounts, Self-Service User Store, and SAML 2.0 Inbound. However, there are no specific version requirements for using these identity sources with CloudAccess. For more information, see the following sections: ◆ Chapter 5, “Configuring Social Identity Sources,” on page 49 ◆ Chapter 6, “Configuring Self-Service Registration and Password Management,” on page 59 ◆ Chapter 7, “Configuring SAML 2.0 Inbound Identity Sources,” on page 65
Client Workstations	**Administration:** Supported workstations for administration tasks: **NOTE:** Administration tasks are not supported on mobile devices. ◆ Microsoft Windows 10.*x*, 8.1, or 7.1 (no touch screens) ◆ Apple OS X (latest version) **Users:** Supported workstations for users: ◆ Microsoft Windows 10.*x*, 8.1, or 7.1 ◆ Apple OS X (latest version) ◆ Chromebooks (latest version)

Components	Requirements
Mobile Devices	**Administration:** Not supported on mobile devices. **Users:** Supported iOS mobile devices for users: ◆ iPhone with iOS 9.*x* or later ◆ iPad or iPad mini with iOS 9.*x* or later Supported Android mobile devices for users: ◆ Android phones and tablets with KitKat 4.4 or Lollipop 5.*x*
Browsers	**Administration:** Supported browsers for administration tasks: ◆ Mozilla Firefox (latest version) on a supported workstation ◆ Google Chrome (latest version) on a supported workstation ◆ Microsoft Internet Explorer 11 on a supported workstation ◆ Apple Safari (latest version) on a supported workstation **NOTE:** You must disable pop-up blockers to access the administration console. If you experience any issues with a supported browser, ensure that you have the latest version of the browser installed, or try another supported browser. Administering the appliance with Internet Explorer might be slower than with other supported browsers. **Users:** Supported browsers for users: ◆ Mozilla Firefox (latest version) ◆ Google Chrome (latest version) ◆ Microsoft Internet Explorer 11 ◆ Apple Safari (latest version)
Email Clients	For email proxy, CloudAccess supports IMAP, POP3, and SMTP across a variety of desktop and mobile email clients. For example, Windows Live Mail 2011 and the latest version of the Apple Mail Client on iPad or iPhone with iOS 9.*x* or later. **NOTE:** The email ports in the CloudAccess cluster cannot be changed. It might be necessary to adjust the mail protocol or port configuration on the email clients to connect to the email proxy.
DNS	CloudAccess requires that all appliance nodes, administration workstations, end-user workstations, mobile devices, and identity sources be able to resolve the public DNS name of the appliance. **NOTE:** The L4 switch must be configured with the publicly resolvable DNS of the cluster before you initialize the appliance.
SaaS Application Requirements	Each SaaS application has different requirements. For more information about the requirements for each SaaS application, see the *CloudAccess Connectors Guide*.

In addition to the product requirements specified in Table 2-2 on page 18, CloudAccess requires specific inbound and outbound ports for communication with other applications and components in your environment. Review the following tables to ensure that the appropriate ports are open in your environment.

The CloudAccess appliance uses the following ports for inbound communication.

Table 2-3 Inbound Ports

Port	Purpose
80	http access, redirects to 443/https
443	◆ End user communication ◆ Administration ◆ Cluster synchronization ◆ Office 365 cloud (Fat client support)
524	Cluster replication

The CloudAccess appliance uses the following ports for outbound communication.

Table 2-4 Outbound Ports

Port	Connects To
389	LDAP **NOTE:** Usually it is either 389 or 636, not both.
636	LDAPS **NOTE:** Usually it is either 389 or 636, not both.
524	Cluster synchronization
443	◆ Cluster members for proxy requests ◆ Windows server where the connector for Office 365 is installed ◆ Advanced Authentication ◆ Salesforce/Google provisioning
514	Syslog
1290	Sentinel Log Manager server
53	DNS lookups
25	Email alerts
123	NTP

Appliance Installation Worksheet

Use the following worksheet to gather the required networking information to install the appliance.

Table 2-5 Appliance Installation Worksheet

	Gather the following information:
❑	Publicly resolvable DNS name for the appliance

	Gather the following information:
□	NTP server
□	DNS server, subnet mask, and gateway
□	(Recommended) An SSL certificate signed by a well-known certificate authority (CA)

Deploying the Appliance

The CloudAccess appliance is an Open Virtualization Format (OVF) virtual appliance. You must deploy the appliance to your VMware or Hyper-V server.

The appliance must obtain an IP address through DHCP or have an assigned static IP address. Two different OVF files for the appliance are available, to accommodate DHCP and non-DHCP environments:

- **DHCP environment:** Use the `*.ovf` file if your environment has a DHCP server.
- **Non-DHCP environment:** Use the `*-vcenter.ovf` file if your environment does not have a DHCP server and you need to use a static IP address.

To deploy the appliance in a VMware environment:

1. Download the appropriate file from the NetIQ Downloads web page (https://dl.netiq.com/).
2. (Conditional) If you are using Windows, extract the VMware image to access the available OVF file.
3. (Conditional) If you are using Linux, use the following command to extract the image:

   ```
   tar -zxvf vmware_image.tar.gz
   ```

4. (Conditional) If you have a DHCP server in your environment, deploy the `*.ovf` file to a specific ESXi host. For more information, see the VMware documentation.
5. (Conditional) If you do not have a DHCP server in your environment:

   5a Deploy the `*-vcenter.ovf` file to a VMware vCenter Server, using either the command line tool `ovftool` or the VMware vSphere client.

   5b Configure the appliance properties, ensuring that you change the `use_dhcp` property to false. Other required properties include the static IP address, subnet mask, default gateway, DNS server, and NTP server name.

   TIP: If you deploy the appliance using the `ovftool`, you can configure the appliance properties from the command line and auto-start the VM so you do not have to use the vSphere client to configure the properties before starting the VM.

6. Power on the appliance, then proceed to "Initializing the Appliance" on page 23.

   The initial boot configures the appliance. This process could take between five and twenty minutes to complete. When the appliance is ready, it displays a welcome message with the initialization URL `https://`*`appliance_ip_address`*`/appliance/Init.html`.

7. Take note of the initialization URL. You will need this address to begin the initialization process.

Upgrading Your Environment

CloudAccess does not support in-place upgrades. However, you can upgrade your existing CloudAccess or SocialAccess environment to CloudAccess 3.0 as follows:

1. Install a new CloudAccess 3.0 appliance.
2. Add the new appliance to your existing cluster.
3. Make the new appliance the master node.
4. Remove the old node.
5. Replace the other nodes in the cluster by adding a new 3.0 node, then removing the old node.

Initializing the Appliance

After you have deployed the appliance, you must initialize it. Use the "Appliance Installation Worksheet" on page 21 to make sure you have the required information before you begin.

1 Verify that your environment meets all requirements listed in "Product Requirements" on page 18.

2 From a supported browser, access the initialization web interface at the URL displayed on the appliance screen after it is deployed.

For example: `https://`*`appliance_ip_address`*`/appliance/Init.html`

IMPORTANT: This URL is case-sensitive, so ensure that you enter the non-variable portions of the URL exactly as illustrated in the example above.

---

3 Follow the prompts in the initialization wizard to provide the information needed to initialize the appliance.

NOTE: The password that you specify in the last step becomes the appliance administrator password. Make a note of this password, since you will need it to log in to the appliance or to re-initialize the appliance.

---

4 Click **Finish**.

A successfully initialized appliance automatically redirects the browser to the administration console login page at `https://`*`appliance_dns_name`*`/appliance/index.html`.

5 Log in with the following administrator user name and password:

User name: appliance.admin (The user name is not case-sensitive, so Appliance.Admin also works.)

Password: The password you set for the appliance in the last step of the initialization process.

6 Proceed with Chapter 3, "Configuring the Appliance," on page 25.

Changing Initialization Settings

You can change the initialization settings at any time if needed. Enter `https://`*`appliance_dns_or_IP_address`*`/appliance/Init.html` in a browser to access the initialization settings page, and log in using the password you specified in the last step of the initialization process.

Whenever you make changes to the appliance, click **Apply** and wait for the appliance to finish applying your changes. Do not attempt to perform any other administration tasks in the console until the gears have stopped spinning on the appliance icon.

3 Configuring the Appliance

After you have installed and initialized the appliance, you can configure the appliance to communicate with the SaaS applications. For more information about initializing the appliance, see "Initializing the Appliance" on page 23.

Getting Started

After you initialize the appliance, the browser automatically redirects you to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`. If the initialization does not automatically redirect you, you can open the page manually to complete the appliance configuration.

To access the administration console:

1. In a supported browser, enter `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Log in using the appliance administrator credentials:

   User name: appliance.admin (The user name is not case-sensitive, so Appliance.Admin also works.)

   Password: The password you set for the appliance in the last step of the initialization process.

Before you begin any configuration tasks, you should register your appliance. For more information, see "Registering the Appliance" on page 26.

After you register the appliance, use the icons at the top of the Admin page to access the other administration pages:

- **Roles:** Configure roles for different users within CloudAccess. For more information, see "Assigning Roles to Users" on page 68.
- **Policy:** Map roles (groups) from the identity source to authorizations for the SaaS applications. For more information, see Chapter 12, "Mapping Authorizations," on page 91.
- **Approval:** Approve or deny authorizations for the SaaS applications. This icon appears only if you have mapped roles to authorizations and selected the option to require approval for accounts, and there are accounts waiting for approval. For more information, see "Approving Requests" on page 95.
- **Reports:** Report on user activities to the SaaS applications. For more information, see Chapter 13, "Reporting," on page 97.
- **Devices:** View and manage registered mobile devices. This icon appears only if you have registered mobile devices. For more information, see "Unregistering Mobile Devices" on page 88.

If your session times out or you log out, the next time you log in to the appliance, CloudAccess displays the page that you last accessed. Admin sessions time out by default after 10 minutes of inactivity, and this setting is not configurable. However, you can adjust the timeout setting for user sessions. For more information, see "Configuring User Session Timeouts" on page 102.

Registering the Appliance

CloudAccess provides a 30-day trial period. If you do not register the appliance within 30 days after installation, the appliance stops working. The bomb icon on the Admin page displays how many days are left in the trial period.

For the purpose of meeting licensing requirements, when you register a single appliance, the cluster as a whole is considered to be registered. However, to use the Customer Center update channel to download and install software updates, you must register each node in the cluster separately. The bomb icon remains on the Admin page if there are nodes in the cluster that have not yet been registered for channel updates. For more information about the update channel, see "Updating the Appliance" on page 104.

To register your appliance:

1. Log in to your Customer Center at https://www.netiq.com/customercenter (https://www.netiq.com/customercenter).
2. Click **Software**.
3. On the Entitled Software tab, click the **Keys** icon.
4. In the pop-up window, select the **Key** value and copy it to the clipboard. You will need this code to register the appliance.
5. (Conditional) If you are not already logged in to the appliance, log in at `https://`*`appliance_dns_name`*`/appliance/index.html`.
6. On the Admin page, click the appliance node, then click **Register appliance**.
7. Enter the email address you used when you registered with the Customer Center.
8. Paste the Key you copied to the clipboard from the Customer Center.
9. Click **Register**.
10. Repeat Step 6 through Step 9 for each appliance in the cluster.

When you have successfully registered all nodes in the cluster, the bomb icon disappears.

Configuring Identity Sources

After you initialize and register your appliance, you can configure one or more identity sources and import users. CloudAccess supports multiple types of identity sources. You can have one or more of each type of identity source configured on your appliance, and you can configure as many identity sources as you need.

The only restrictions are as follows:

- The source for each identity source must be unique. For example, do not configure multiple instances of an identity source for the same Active Directory domain.
- Every user account across the different identity sources must be unique.

NOTE: The initial import of a large number of users can take several hours, and you must allow the import process to finish before you try to perform other appliance configuration tasks or configure any application connectors.

For more information about identity sources, see the following:

- Chapter 4, "Configuring LDAP and JDBC Identity Sources," on page 37

- Chapter 5, “Configuring Social Identity Sources,” on page 49
- Chapter 6, “Configuring Self-Service Registration and Password Management,” on page 59
- Chapter 7, “Configuring SAML 2.0 Inbound Identity Sources,” on page 65

Configuring Networking Options and Certificates

CloudAccess contains a manual routing table, supports two Network Interface Cards (NICs), and provides a forward proxy. The forward proxy is intended only for testing purposes.

- “Configuring the Forward Proxy” on page 27
- “Configuring the Second Network Interface” on page 27
- “A Sample Network Configuration” on page 28
- “Configuring the Routing Table” on page 29
- “Changing the Certificates on the Appliance” on page 29

Configuring the Forward Proxy

The forward proxy takes requests from the internal network and forwards these requests to the Internet.

NOTE: The forward proxy is intended only for testing purposes, and is not supported in a production environment.

To configure the forward proxy:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Drag the **Forward Proxy** icon from the **Tools** palette to the **Tools** panel.
3. Use the following information to configure the forward proxy:

   Forward Proxy Server: Specify the IP address and port number for your proxy server.

   Ignore List: Specify any IP addresses with the associated DNS names that you want the forward proxy to ignore. For example, `127.0.0.0|localhost`. Wildcard entries are not supported in this field.
4. Click **OK** to save your changes. Note that clicking **OK** causes the services to restart and you must log in to the appliance again.

Configuring the Second Network Interface

CloudAccess supports two Network Interface Cards (NICs) for each node in the cluster. You can configure one NIC for the administrative network and a second NIC for the public network. Whether the nodes in a cluster each have one or two NICs configured, the cluster itself has only two DNS names: one for the Admin NICs and one for the Public NICs.

IMPORTANT: If you configure two NICs on one appliance, you must configure all other nodes in the cluster with two NICs.

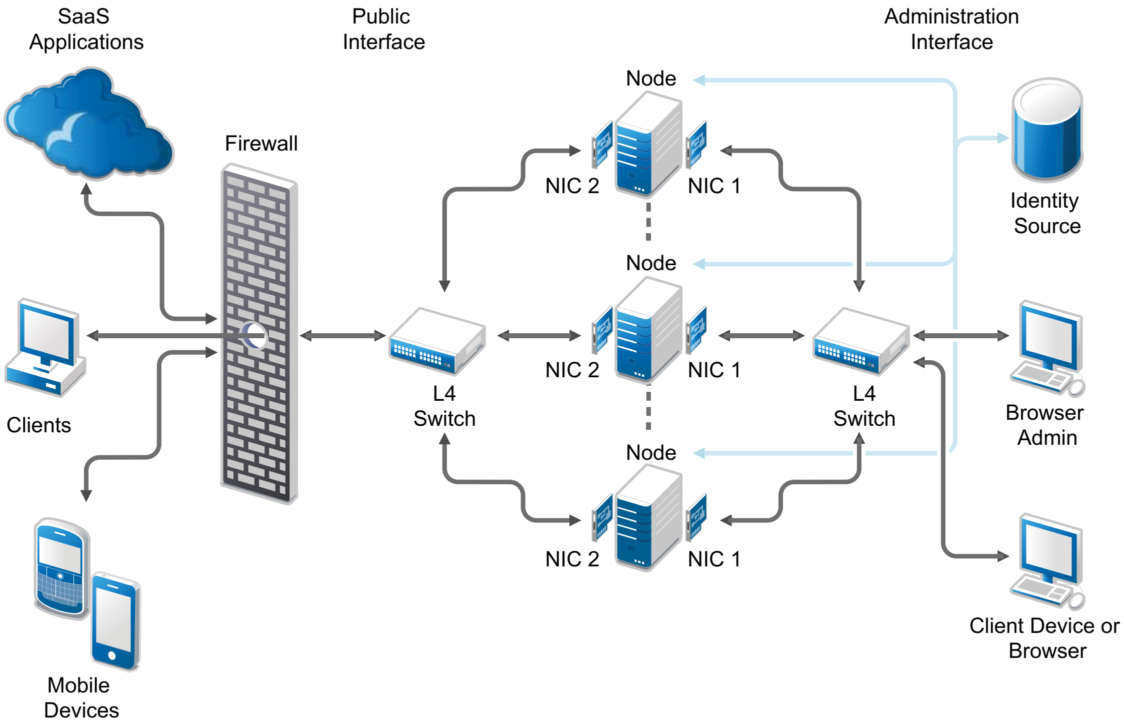
To configure the second NIC on a node:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click a node icon, then click **Configure**.
3. Click the **Public Interface** tab.
4. Select **Enable Separate Public Interface**.
5. Configure the network settings for your public network and click **OK**.
6. (Conditional) If this is the first node in the cluster with a Public NIC, type the DNS name for the public network. Modify the keypairs for SSL and SAML as needed and click **OK**.
7. Click **Apply** to save the changes.
8. Click **Close**.
9. Repeat Step 2 through Step 8 for each node in the cluster.

A Sample Network Configuration

The following graphic depicts a possible network configuration using CloudAccess with both NICs enabled on each node.

***Figure 3-1** A Sample Network Diagram*



The network diagram shows that each node has both NICs enabled. The first NIC is the administration interface for the node and the second NIC is the public interface of the node. All of the administration and corporate information stays on the administration interface side of the network. All user requests and application requests communicate only on the public interface. This configuration provides a layer of security for your corporate information.

Configuring the Routing Table

CloudAccess provides a routing table for your use if your network has static routes. The routing table allows you to define the next hop in your network for the node in the cluster to reach the appropriate destination.

To configure the routing table for each node:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click the node icon, then select **Configure**.
3. Click the **Routing** tab.
4. Specify the appropriate **Reverse Path Filter** setting.

   Reverse path filtering is used to prevent packets that arrived through one interface from leaving through a different interface. If you are in doubt, leave the default setting of **Strict mode**, because it prevents users from spoofing IP addresses from local subnets and reduces the likelihood of distributed denial-of-service (DDoS) attacks.
5. Click the plus sign (+) to add a route.
6. Define the appropriate route, then click **OK**.
7. (Optional) Add additional routes.
8. Click **Close**.
9. Repeat Step 2 through Step 8 for each node in the cluster.

Changing the Certificates on the Appliance

The appliance contains SSL and SAML self-generated certificates, by default both named ag4csrv1, but we highly recommend that you replace the default certificates with signed certificates from a well-known Certificate Authority. The required format for importing a key pair is `.pfx`. This format contains the private key, certificate, and trusted roots required to import.

To change the certificates:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click the cluster icon under **Appliances**, then click **Configure**.
3. Delete the default key pairs by clicking the red delete (X) icon next to the SSL key pair and the SAML key pair.
4. Browse to and select the certificates you want to use, then click **OK**.
5. In the Instructions window, click **OK**.
6. Click **Apply** and wait for the configuration changes to be applied to the appliance. Do not perform other administration tasks in the console while the changes are being applied.
7. Close your browser and reopen it to start a new session using the new key pairs.

Expired key pair certificates prohibit changes from being made to this page and make the key pair field red. If the key pair expires, you must re-initialize the appliance before you can upload a new certificate. For more information, see “Initializing the Appliance” on page 23.

Configuring Clustering

You can cluster the CloudAccess appliance. By default, it is a single node cluster, but CloudAccess supports up to a five-node cluster. The first node in a cluster automatically becomes the master node, but you can change this at any time. You add a node to an existing cluster by selecting **Join Cluster** during the initialization process.

- "Advantages of Clustering" on page 30
- "Adding Nodes to the Cluster" on page 30
- "Promoting a Node to Master" on page 31
- "Removing a Node from the Cluster" on page 32
- "Configuring an L4 Switch for Clustering" on page 32

Advantages of Clustering

Clustering in CloudAccess offers several advantages. Most of these advantages are available only if you configure an L4 switch or Round-robin DNS. The L4 switch is the best solution.

Disaster Recovery: Adding additional nodes to the cluster provides disaster recovery for your appliance. If one node stops running or becomes corrupt, you can promote another node to master.

High Availability for Authentications: CloudAccess provides high availability for authentications and the single sign-on service, when using an L4 switch in conjunction with clustering. This solution allows users to authenticate in case of problems with the nodes within the cluster. The L4 switch sends authentication requests to the nodes with which it can communicate.

Load Balancing: You can configure the L4 switch to distribute authentications to nodes so one node does not receive all authentication requests while other nodes sit idle.

Scalability: Configuring an L4 switch with clustering increases the scalability of CloudAccess. Each node in the cluster increases the number of possible concurrent logins.

Adding Nodes to the Cluster

CloudAccess supports up to five nodes in a cluster. You add nodes to the cluster through the initialization process, and perform all other initialization tasks on the Admin page.

IMPORTANT: If you are using an L4 switch, ensure that you add the first node of the cluster to the L4 switch before initializing the node. Do not add any other nodes to the L4 until the node has fully joined the cluster.

To add a node to the cluster:

1. Verify that the cluster is healthy.
   - All nodes must be running and communicating.
   - All components must be in a green state.
   - All failed nodes must be removed from the cluster.

   For more information about verifying that your cluster is healthy, see "Troubleshooting Different States" on page 109.
2. Download and deploy a new virtual machine (VM) for the new node.

   For more information, see "Deploying the Appliance" on page 22.

3 Initialize the appliance. Select **Join Cluster** as the first step to initialize the new node, then follow the on-screen prompts.

For more information, see "Initializing the Appliance" on page 23.

When initialization is complete, the browser is redirected to `index.html` and a login page appears.

4 Log in to `index.html` and verify that the new appliance appears in the cluster. Wait until all spinner icons stop processing and all components are green before performing any other tasks.

The cluster is adding the node and there are several background processes running. This final step could take up to an hour to complete.

5 After the node is added to the cluster, register the node. For more information, see "Registering the Appliance" on page 26.

Promoting a Node to Master

The first node that you install is the master node of the cluster by default. The master node runs provisioning, reporting, approvals, and policy mapping services. You can promote any node in a cluster to become the master node.

To promote a node to master:

1 Verify that the cluster is healthy.

- All nodes must be running and communicating.
- All components must be in a green state.
- All failed nodes must be removed from the cluster.

For more information about verifying that your cluster is healthy, see "Troubleshooting Different States" on page 109.

2 Verify that all nodes in the cluster are running the same version of CloudAccess. If any nodes need to be updated, ensure that you update the nodes *before* you switch the master node. For more information, see "Updating the Appliance" on page 104.

3 Take a snapshot of the cluster.

4 Click the node to become the master node on the Admin page, then click **Promote to master**.

An M appears on the front of the node icon indicating it is now the master node. This process might take a while to complete. Watch for the node spinner icons to stop and Health indicators to turn green before proceeding with any additional configuration changes.

The services move from the old master to the new master. The old master is now just a regular node in the cluster.

WARNING

- If the old master node is down when you promote another node to master, remove the old master from the cluster, then delete it from the host server. Otherwise, the appliance sees two master nodes and becomes corrupted.
- When you switch the master node, the logs start again on the new master and reports start again on the new master. The historical logs are lost. The reporting data is also lost, unless you are using Sentinel Log Manager. For more information, see "Integrating with Sentinel Log Manager" on page 97.

Removing a Node from the Cluster

You can remove a node from the cluster if something is wrong with the node. However, ensure that you use the following steps to properly remove the node. If you simply delete a node from the cluster, the appliance deletes the node from the interface, but the virtual image still exists and continues to run. Leaving the virtual image running allows users to authenticate to a node that does not exist on the Admin page.

NOTE: After you remove a node, you cannot add the same VM instance back into the cluster. You must delete this instance of the appliance from your host server, then deploy another instance to the host server to add a node back into the cluster.

To remove a node from the cluster:

1. (Conditional) If the node you are removing is the master node, promote another node to be master before you remove the old node. For more information, see "Promoting a Node to Master" on page 31.
2. (Conditional) If you are using an L4 switch, delete the node from the L4 switch. For more information, see the L4 switch documentation.
3. On the Admin page, click the node you want to remove from the cluster.
4. Click **Remove from cluster**.

   The Admin page immediately shows that the node is gone, but it takes some time for the background processes to finish.
5. Stop the virtual image on the host server, and then delete the instance of the node from the host server.

Configuring an L4 Switch for Clustering

If you want high availability or load balancing, you must configure an L4 switch for the CloudAccess appliance. An L4 switch can be configured in many different ways. Use the following recommendations to configure the L4 switch to work with the appliance:

- **Heartbeat:** Use the following URL to define the heartbeat for the L4 switch:

  ```
  https://appliance_ip_address/osp/h/heartbeat
  ```

  The L4 switch uses the heartbeat to determine if the nodes in the cluster are running and working properly. The heartbeat URL returns a text message of Success and an HTTP 200 response code.
- **Persistence:** Also known as **sticky sessions**, persistence allows all subsequent requests from a client to be sent to the same node. To make this happen, select SSL session ID persistence when configuring the L4 switch.

Session persistence ensures that the same real server is used for the CloudAccess login and the subsequent application single sign-on. Using the same server allows caching for a series of related transactions, which can improve the server performance and reduce the latency of transactions. It removes the delay that might occur if the client sends a request to a new node instead of using the existing session to the same node. To ensure that transactions for the same client are forwarded to the same real server in a load-balanced cluster configuration:

- You can set the L4 switch to use IP-based persistence, which uses the user device's IP address to maintain an affinity between the user session and the same real server in the cluster. IP-based persistence fails if a user's device IP address changes between requests, such as if a user's mobile device changes networks during a session. It also fails if all user devices come through a proxy service where all transactions appear to come from the same IP address.
- You can set the L4 switch to use sticky-bit persistence. However, note that sticky-bit persistence is problematic for L4 switches that do not support stickiness. Sticky sessions also do not work with browsers set to disable cookies.
- You can use a proxy approach for the identity provider nodes that does not depend on the L4 configuration. However, this solution can quickly become chatty.

Configuring an L4 Switch for Email Proxy

CloudAccess contains an email proxy for users with Google Apps that supports three protocols: SMTP, POP3S, and IMAPS. You must configure your L4 switch to handle these protocols. Use the following high level steps to configure the protocols for your L4 switch. For more information, see your specific L4 documentation.

- "Configuring the SMTP Protocol Handler" on page 33
- "Configuring the POP Protocol Handler" on page 34
- "Configuring the IMAP Protocol Handler" on page 34

Configuring the SMTP Protocol Handler

To configure an SMTP protocol handler for your L4 switch:

1. On your L4 switch, configure a new IP group (traffic group) or use an existing group for the virtual servers in the L4 switch.

   You can use this group for all of the protocols.

2. (Optional) Create a health monitor:

   2a Set the health checking for the pool to **TCP transaction monitor**.

   2b Set the timeout to 30 seconds.

   2c Set the health monitor to separately monitor each node.

3. Create a traffic pool for the SMTP virtual server to use:

   3a Add each appliance node to the pool using the IP address with the port.

   For example: 192.168.1.14:25. The SMTP port is 25.

   3b (Optional) Add the health monitor created in Step 2.

   3c Select your load balancing settings.

   For example: round robin or random

   3d Set the session persistence to **SSL Session ID**.

4 Create a new virtual server:

4a Specify the protocol as SMTP and the port as 25.

4b Use the traffic group defined in Step 1 and the pool defined in Step 3 for the virtual server.

5 Start the virtual server.

Configuring the POP Protocol Handler

To configure a POP protocol handler for your L4 switch:

1 On your L4 switch, configure a new IP group (traffic group) or use an existing group for the virtual servers in the L4 switch.

You can use this group for all of the protocols.

2 (Optional) Create a health monitor:

2a Set the health checking for the pool to **TCP transaction monitor**.

2b Set the timeout to 30 seconds.

2c Set the health monitor to separately monitor each node.

3 Create a traffic pool for the POP virtual server to use:

3a Add each appliance node to the pool using the IP address with the port.

For example: 192.168.1.14:995. The POP port is 995.

3b (Optional) Add the health monitor created in Step 2.

3c Select your load balancing settings.

For example: round robin or random

3d Set the session persistence to **SSL Session ID**.

4 Create a new virtual server:

4a Specify the protocol as SSL (POP3S) and the port as 995.

4b Use the traffic group defined in Step 1 and the pool defined in Step 3 for the virtual server.

5 Start the virtual server.

Configuring the IMAP Protocol Handler

To configure an IMAP protocol handler for your L4 switch:

1 On your L4 switch, configure a new IP group (traffic group) or use an existing group for the virtual servers in the L4 switch.

You can use this group for all of the protocols.

2 (Optional) Create a health monitor:

2a Set the health checking for the pool to **Connect**.

2b Set the health monitor to separately monitor each node.

3 Create a traffic pool for the IMAP virtual server to use:

3a Add each appliance node to the pool using the IP address with the port.

For example: 192.168.1.14:993. The IMAP port is 993.

3b (Optional) Add the health monitor created in Step 2.

3c Select your load balancing settings.

For example: round robin or random.

3d Set the session persistence to **SSL Session ID**.

4 Create a new virtual server:

4a Specify the protocol as SSL (IMAPS) and the port as 993.

4b Use the traffic group defined in Step 1 and the pool defined in Step 3 for the virtual server.

5 Start the virtual server.

4 Configuring LDAP and JDBC Identity Sources

CloudAccess supports the use of various identity sources for authenticating users and for provisioning accounts to the SaaS applications. After initializing the appliance, you can configure one or more identity sources on the Admin page of the administration console. In addition to LDAP and JDBC database identity sources that are capable of importing users and provisioning them to SaaS applications, CloudAccess supports many other non-provisioning identity sources such as social media identity sources (Facebook, LinkedIn, etc.), the Self-Service User Store (SSUS), and SAML 2.0 Inbound (SAML2 In).

This chapter provides information about LDAP and JDBC identity sources that cache and provision user accounts. For information about other identity sources, see the following:

- Chapter 5, “Configuring Social Identity Sources,” on page 49
- Chapter 6, “Configuring Self-Service Registration and Password Management,” on page 59
- Chapter 7, “Configuring SAML 2.0 Inbound Identity Sources,” on page 65

Understanding LDAP Identity Sources

For CloudAccess to provision user accounts to the SaaS applications, each user account in the identity source must contain the attributes listed. If you are using an LDAP identity source, there are specific attributes that must be populated on the user accounts. If you are using a JDBC database, there are certain columns of information that must be populated. The information for each identity source is different.

NOTE: For security reasons, by default CloudAccess does not allow you to add a user with a user name that is the same as a previously added user. If you attempt to do so, CloudAccess displays the user as not activated. For more information, see “Troubleshooting Provisioning Issues” on page 114.

Review the information in the following sections before you deploy the appliance and when you configure additional identity sources. Ensure that your identity source meets all requirements and the user account information in the identity source contains the proper information to synchronize the accounts.

- “Active Directory Requirements” on page 37
- “eDirectory Requirements” on page 38
- “Understanding LDAP Advanced Options” on page 39

Active Directory Requirements

Verify that your Active Directory environment meets the following requirements:

❐ Windows Server 2012 R2 or Windows Server 2008 R2.

❐ A unique identity for each user account, whether you have one or more domains or identity sources. The appliance uses the sAMAccountName as the unique identifier for the users.

To provision user accounts from Active Directory to the SaaS applications, all of the following attributes must be populated on the Active Directory users:

- First name
- Last name
- Full name (**Display name** is the field that populates this attribute.)
- sAMAccountName or Logon Name (Pre-Windows 2000)
- User Principal Name (UPN)
- Email address

Obtain the following required items:

- The password and the fully distinguished LDAP-formatted name of a user in Active Directory who has read access to the user objects. The appliance will use this user account to make LDAP binds to Active Directory.
- The IP address of one or more Active Directory servers that contain the users.
- The context of the users in Active Directory.

eDirectory Requirements

Verify that your eDirectory environment meets the following requirements:

- ❒ eDirectory LDAP 8.8.8.
- ❒ A unique identity for each user account, whether you have one or more eDirectory trees or identity sources.

To provision user accounts from eDirectory to the SaaS applications, all of the following attributes must be populated on the eDirectory users:

- CN (**Username** is the field that populates this attribute.)
- Given Name (**First name** is the field that populates this attribute.)
- Internet EMail Address
- Surname (**Last name** is the field that populates this attribute.)

Obtain the following required items:

- The password and fully distinguished LDAP-formatted name of a user in eDirectory who has the following rights. The appliance will use this user account to make LDAP binds to eDirectory:
    - **Property Rights**
        - **CN:** compare, read, inherit
        - **Description:** compare, read, inherit
        - **Given Name:** compare, read, inherit
        - **GUID:** compare, read, inherit
        - **Internet EMail Address:** compare, read, inherit
        - **Login Disabled:** compare, read, inherit
        - **Member:** compare, read, inherit
        - **Group Membership:** compare, read, inherit
        - **Surname:** compare, read, inherit

    - **Entry Rights:** browse, inherit
- The IP address of one or more eDirectory servers that contain a replica of the partition holding the user objects and that run NLDAP.
- The context of the users in eDirectory.

Understanding LDAP Advanced Options

The connector for Active Directory and the connector for eDirectory contain predefined behaviors for importing, matching, and provisioning users. You can override the default behavior of the connectors for LDAP identity sources through the Advanced Options for the connectors in the administration console. For example, if you have a large number of users or groups and you want to import only a subset of those users and groups, you can use the Advanced Options to filter them to a set of users and groups you want imported.

By default, CloudAccess uses an internal unique attribute to match users and to provision users to the connected systems. For more information about provisioning, see “Troubleshooting Provisioning Issues” on page 114.

NOTE: The connectors for the LDAP identity sources change all of the keys and values in the filter fields to lowercase. It is best to use a case-ignore attribute.

Identity source search polling rate every: Select how often you want the connector for the LDAP directory to poll the LDAP identity source for changes. By default, the rate is every minute.

Filter extension: Specify a filter for the object class and attribute you want to use to import users. If users do not meet the criteria defined in the filter, CloudAccess does not import those users.

For example, `(&(objectclass=user)(samaccountname=abc*))` imports only users that start with the samaccountname of `abc*`.

Identity source LDAP attribute to use for imported accounts: Specify the LDAP attribute that the connector uses as the naming attribute (login name) when importing accounts from the identity source.

Allow unmapped users to authenticate: Select whether to allow users to authenticate that have not been imported to CloudAccess, because they have been excluded by the filter extension. The unmapped users must use an email address to log in. These users can still log in to the User portal page, but will see only public appmarks.

Override default group filter: Select whether to override the default group filter so you can limit which groups the connector for the LDAP identity source imports to CloudAccess. If you select this option, you must specify a correct filter.

For example, `(&(objectclass=group)(cn=custom*))` allows only groups with a CN that start with `custom*`.

NOTE: When you configure a filter extension for an eDirectory identity source, user objects in the external eDirectory identity store that do not match the filter are not imported into CloudAccess. If you also enable the option **Allow unmapped users to authenticate**, unmapped users can use Basic SSO type connectors, but they cannot store or play back their credentials for single sign-on later because their user objects do not actually exist in CloudAccess.

Attribute mappings: Click **Default** to view the default mappings that CloudAccess makes between the identity sources and the connected systems. The attributes on the left are the attributes for CloudAccess. The attributes on the right are for the LDAP directory.

(Optional) Above the default attributes, you can map five attributes to five custom attributes in CloudAccess. To map the LDAP directory attribute, specify the attribute name in the field next to the custom attribute, then click **OK** and **Apply** to save the changes.

NOTE: Similar to the CN attribute that must be unique for each user, if you configure custom attribute matching, the value of each custom attribute must also be unique.

Relaxed user matching: By default, CloudAccess matches users using an internal unique ID. This option changes the appliance to match users by the CN or sAMAccountName attributes.

Use this option when you want to recreate previously deleted users so CloudAccess can manage the users again. However, ensure that you do not create different users with the same CN or sAMAccountName as previously deleted users. Otherwise, those users will have access to the previously deleted users' cloud application data.

Understanding JDBC Identity Sources

For CloudAccess to provision user accounts to the SaaS applications, each user account in the identity source must contain the attributes listed. If you are using a JDBC database, there are certain columns of information that must be populated.

NOTE: To use the JDBC database as an identity source, you must know and understand JDBC databases. The information provided in this section is intended for database administrators.

Review the information in the following sections and ensure that your identity source meets all requirements and the user account information in the identity source contains the proper information to synchronize the accounts.

- "JDBC Requirements" on page 40
- "Obtaining the Script Files" on page 41
- "Populating the Required Columns" on page 41
- "Dataflow Information" on page 42

JDBC Requirements

Before you use a JDBC database as an identity source, ensure that you have a supported type of JDBC database. For more information, see "Product Requirements" on page 18.

Obtain the following information:

- The IP address of the JDBC database.
- The port for communication. The default port is 1433 for Microsoft SQL Server or 1521 for Oracle Database.
- The database name or sid. (`idm` for Microsoft SQL Server defined as the `sid` in Oracle Database).
- The password for the user name in the sample scripts you install. The script files must be installed before you can configure a JDBC database as an identity source. For more information, see "Obtaining the Script Files" on page 41.

Obtaining the Script Files

To use JDBC as an identity source, you must install script files on your JDBC database so CloudAccess knows what tables to read to access the users and groups information. You can download the scripts when you configure JDBC as an identity source. You download a single zipped file that contains multiple scripts.

The different scripts are:

- **indirect_install:** Installs the schema, which includes the indirect tablespace and `proc_authuser ()` stored procedure, as well as the automatic triggers for the `indirect.user` and `indirect.grp` tables.
- **copy_from:** Copies user account information from the database default user store into the `indirect.usr` table for processing by the connector for JDBC.
- **uninstall:** Removes the schema and deletes or drops the connector user accounts in the underlying database.

Populating the Required Columns

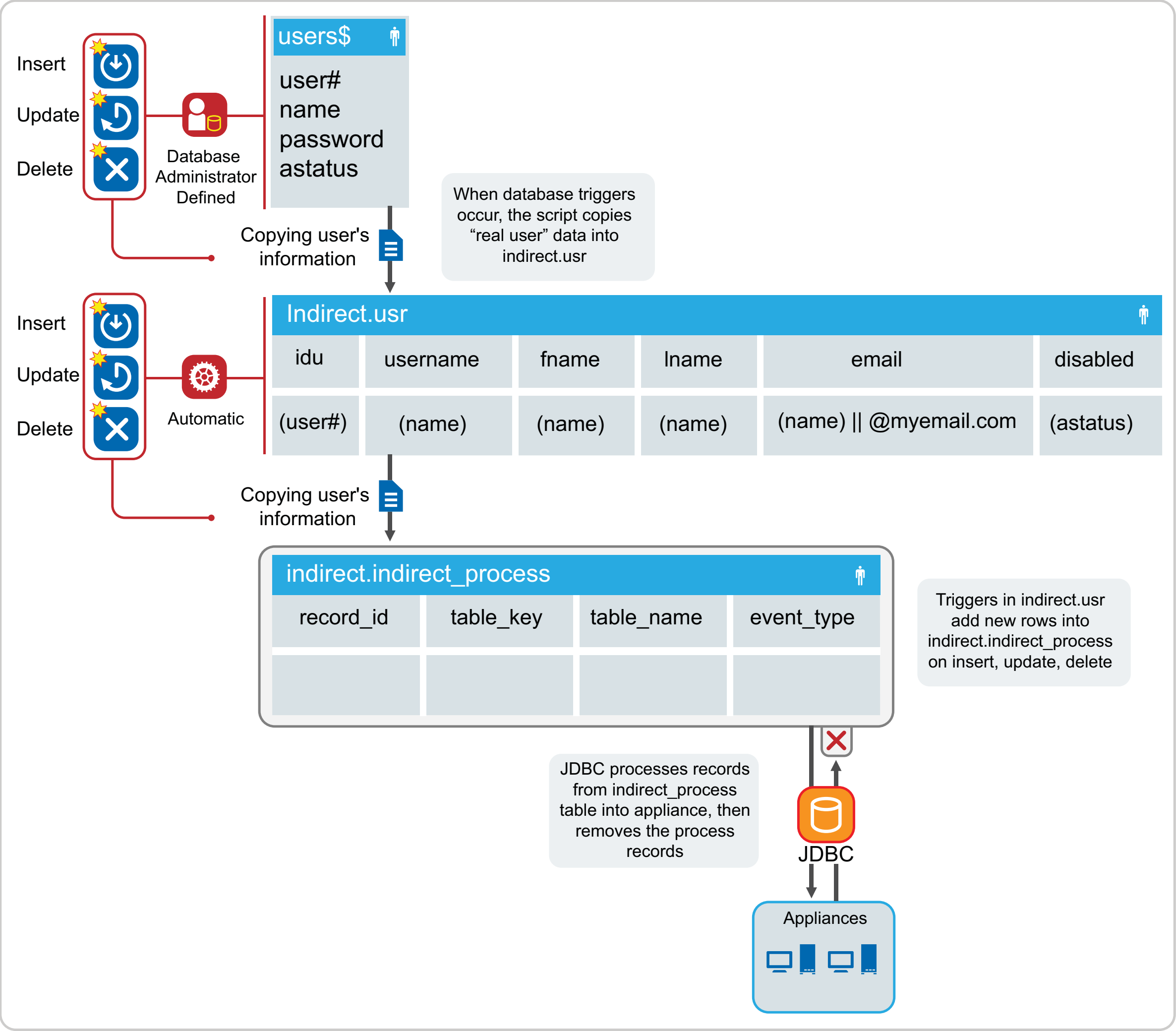
To provision users from the JDBC database to the SaaS applications, you must have the following columns populated for each user account in the JDBC database:

- `indirect.usr.idu`
- `indirect.usr.username`
- `indirect.usr.fname` (Mandatory only for Google Apps accounts)
- `indirect.usr.lname`
- `indirect.usr.email` (Mandatory only for Salesforce accounts)

Dataflow Information

The connector for JDBC uses indirect tables to gather the needed information, ensuring that the appliance does not work directly with the information in the database. The following graphic depicts how the connector for JDBC obtains the information from the JDBC database. This process is the same regardless of the type of database to which the appliance connects.

***Figure 4-1** Dataflow of User Information*


Insert
Update
Delete
Database Administrator Defined
Copying user's information
Insert
Update
Delete
Automatic
Copying user's information
JDBC
Appliances

users$
user#
name
password
astatus

When database triggers occur, the script copies “real user” data into indirect.usr

Indirect.usr					
idu	username	fname	lname	email	disabled
(user#)	(name)	(name)	(name)	(name) || @myemail.com	(astatus)

indirect.indirect_process			
record_id	table_key	table_name	event_type

Triggers in indirect.usr add new rows into indirect.indirect_process on insert, update, delete

JDBC processes records from indirect_process table into appliance, then removes the process records

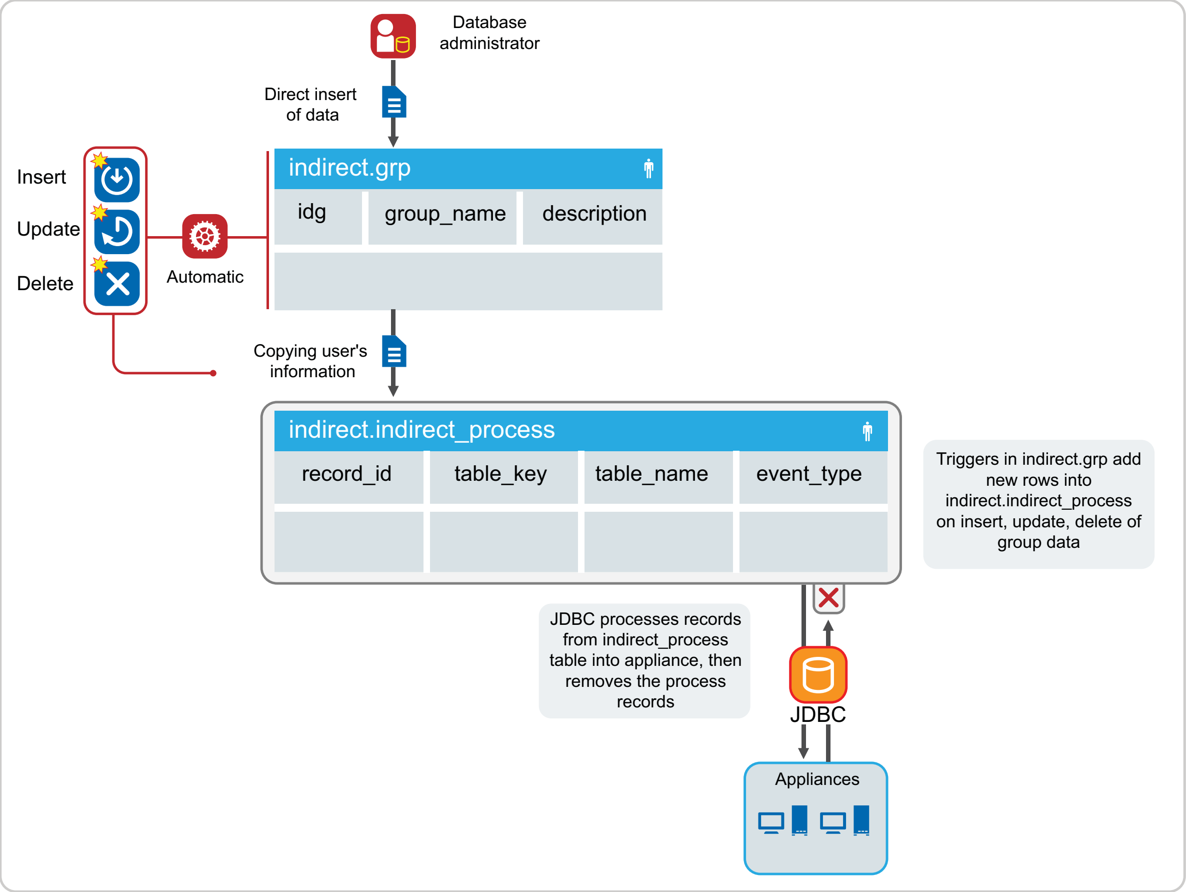
The database administrator creates the user accounts or logs in to the `user$` table. (The dataflow figures are based on the default Oracle security table `user$`.) The database administrator defines triggers or procedures that copy information into the `indirect.usr` table.

The `indirect_install` SQL script creates the automatic insert, update, or delete triggers on the `indirect.usr` table. When rows in the `indirect.usr` table are altered, the automatic triggers add a row to the `indirect.indirect_process` table.

The appliance polls the `indirect.indirect_process` table. When the appliance detects rows in the `indirect.indirect_process` table of type `user`, the appliance adds, modifies, or deletes the user account in the applications connected to the appliance.

The appliance then deletes the row from the `indirect.indirect_process` table after the appliance processes the information.

Figure 4-2 *Dataflow of Group Information*

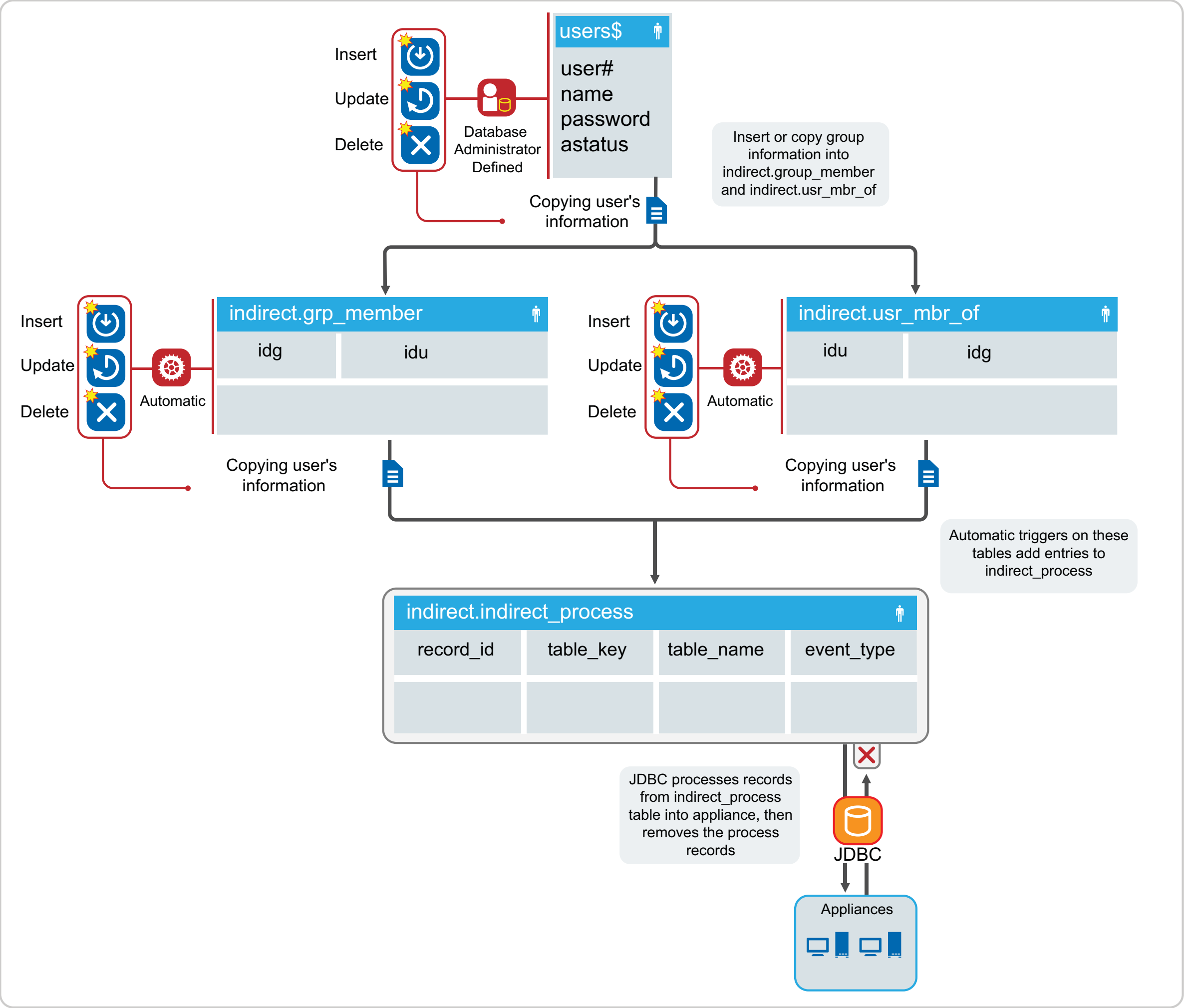

Database administrator
Direct insert of data
Insert
Update
Delete
Automatic
indirect.grp
idg
group_name
description
Copying user's information
indirect.indirect_process
record_id
table_key
table_name
event_type
Triggers in indirect.grp add new rows into indirect.indirect_process on insert, update, delete of group data
JDBC processes records from indirect_process table into appliance, then removes the process records
JDBC
Appliances

The database administrator performs a direct or triggered insert of data into the `indirect.grp` table.

The `indirect_install` SQL script creates the automatic insert, update, or delete triggers on the `indirect.grp` table. When rows in `indirect.grp` are altered, the automatic triggers add a row to the `indirect.indirect_process` table.

When the appliance detects rows in the `indirect.indirect_process` table of type group, the appliance adds, modifies, or deletes the groups in the applications connected to the appliance. The appliance then deletes the row from the `indirect.indirect_process` table after the appliance processes the information.

Figure 4-3 Relationship between Users and Groups


Insert
Update
Delete
Database Administrator Defined
users$
user#
name
password
astatus
Copying user's information
Insert or copy group information into indirect.group_member and indirect.usr_mbr_of
Insert
Update
Delete
Automatic
indirect.grp_member
idg
idu
Copying user's information
Insert
Update
Delete
Automatic
indirect.usr_mbr_of
idu
idg
Copying user's information
Automatic triggers on these tables add entries to indirect_process
indirect.indirect_process
record_id
table_key
table_name
event_type
JDBC processes records from indirect_process table into appliance, then removes the process records
JDBC
Appliances

The indirect schema does not have a direct concept of group membership, but maintains a relationship between the `user idu` column and the `group idg` column in the `indirect.grp_member` and `indirect.usr_mbr_of` tables.

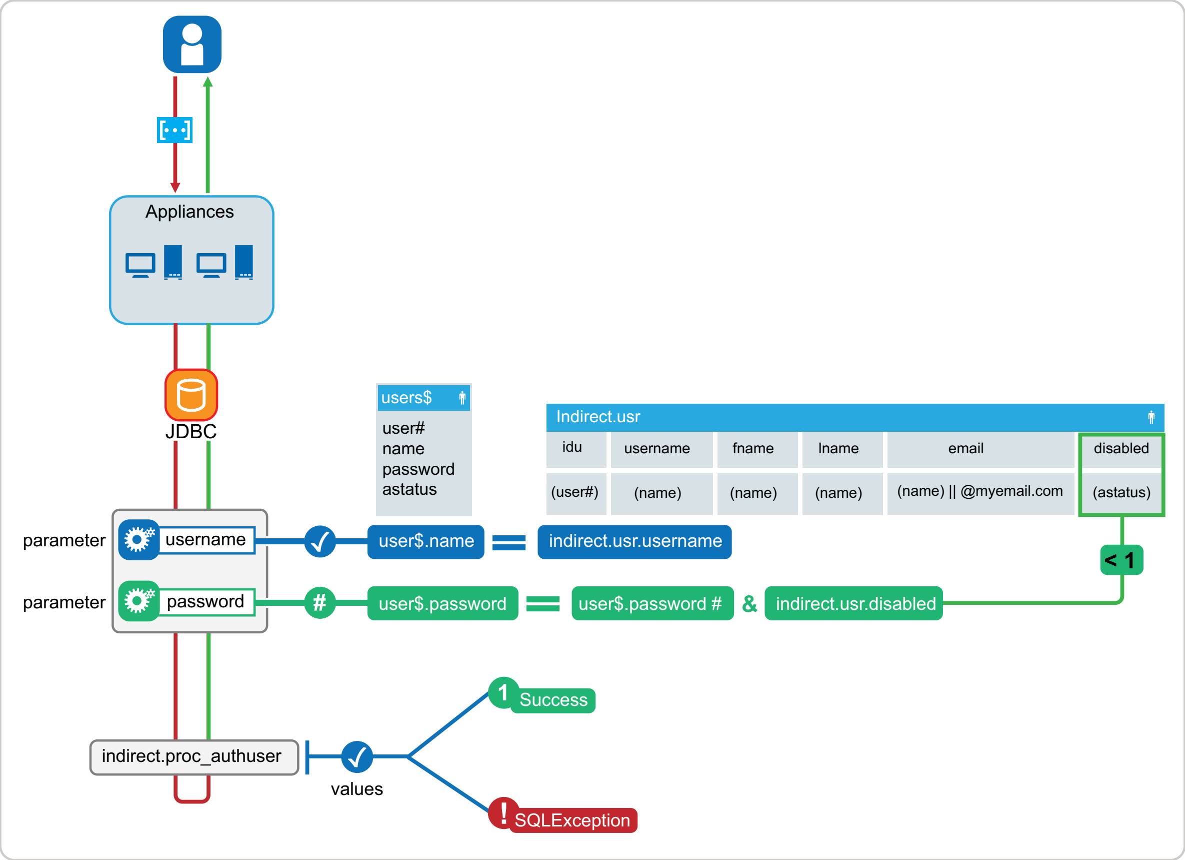
For group membership, the desired group `idg` and user `idu` must exist in both tables. The `indirect_install` SQL script creates the automatic insert, update, or delete triggers on the `indirect.grp_member` and `indirect.usr_mbr_of` tables. When rows in these tables are altered, the automatic triggers add a row to the `indirect.indirect_process` table.

When the appliance detects rows in the `indirect.indirect_process` table for group membership, the appliance adds, modifies, or deletes the group memberships in the applications connected to the appliance. The appliance then deletes the row from the `indirect.indirect_process` table after the connector processes the information.

For example, if the administrator wants to add a user with `idu 6` to a group with `idg 10`, the administrator would have to manually (or through triggers) add entries into both the `grp_member` and `usr_mbr_of` tables.

```
"INSERT INTO indirect.grp_member(idg,idu) VALUES(10,6); INSERT INTO
indirect.usr_mbr_of(idu,idg) VALUES(6,10);”
```

Figure 4-4 Authentication Process



To verify authentication credentials, the appliance calls a stored procedure `indirect.proc_authuser` with the parameters of `@username,@password`. The procedure compares the `username` parameter with the default user table (`user$`) and the `indirect.usr.username` fields. If they match, the process checks the `indirect.usr.disabled` flag (disabled > 0 = disabled). If login is enabled (disabled = 0), the process compares the `password` parameter to the existing password hash in the `user$` table. If the password hash matches, the process authenticates the user successfully. If any of these conditions are not met, the process returns a `SQLException` to the appliance, and authentication fails.

You can alter the stored procedure based on the desired schema that the database administrator wishes to use for authentication. Keep in mind that the stored procedure `indirect.proc_authuser(@username,@password)` is hard-coded into the appliance, and expects either a `success (1)` or `SQLException` returned.

Configuring an LDAP or JDBC Identity Source

You can configure as many identity sources as you want. However, all of the user IDs across the different identity sources must be unique. If necessary, you can also change configuration information for an identity source that you previously set up.

NOTE: Although CloudAccess allows you to modify an existing eDirectory or Active Directory connector to point to a different tree, we do not recommend this approach because it can result in inconsistent display of user and group data. If you want to point a connector to a different tree, delete the existing connector and create a new connector that points to the correct tree.

To configure an LDAP or JDBC identity source:

1. Ensure that your identity source meets all requirements and the user account information in the identity source contains the proper information to synchronize the accounts. For more information, see "Understanding LDAP Identity Sources" on page 37 or "Understanding JDBC Identity Sources" on page 40.
2. Log in with an appliance administrator account to the administration console at

   `https://`*`appliance_dns_name`*`/appliance/index.html`
3. (Conditional) If you are configuring a new identity source, drag the connector for the identity source from the **Identity Sources** palette to the **Identity Sources** panel.
4. (Conditional) If you are changing the settings for an existing identity source, click the identity source icon in the **Identity Sources** panel, then click **Configure**.
5. (Conditional) If you are configuring the connector for Active Directory or eDirectory, provide the following information:

   Credentials: Specify the fully distinguished LDAP format name and password of the Active Directory administrator account or the eDirectory administrator account with the minimum rights.

   Search Context: Specify the fully distinguished LDAP format of the context where the connector searches for user objects.

   Active Directory Servers: Specify the IP address and LDAP port of the Active Directory server where the user objects reside. Select **Enable LDAP SSL** to use port 636. Otherwise, the default non-SSL port is 389.

   eDirectory Server: Specify the IP address and LDAP port of the eDirectory server that contains a Master or Read/Write replica of the partition where the user objects reside. Select **Enable LDAP SSL** to use port 636. Otherwise, the default non-SSL port is 389.
6. (Optional) Configure the appropriate LDAP Advanced Options. For more information, see "Understanding LDAP Advanced Options" on page 39.
7. (Conditional) If you are configuring the connector for JDBC, provide the required information for your MS-SQL or Oracle database, and accept the 3rd-party JDBC license agreement. For more information, see "JDBC Requirements" on page 40.
8. (Conditional) The **Enable local vault caching** option is required for provisioning users to the SaaS applications (Google Apps, Salesforce, ServiceNow, and Office 365) and is selected by default. If you are not configuring the identity source to be used with SaaS applications, deselect this option. If local caching is not enabled, users are not imported, but you can still use the LDAP and JDBC identity sources as authentication sources only.
9. Click **OK** to save the configuration information.
10. Click **Apply** to commit the changes to the appliance.

As users in the search contexts from the identity source are imported and activated, the Admin page displays user count activity on the **Users** bar. Ensure that the import process completes before you try to configure any application connectors or make any other changes in the administration console.

IMPORTANT: The initial import of a large number of users (for example, 20,000 or more) from the identity source can take several hours, and the administration console does not currently provide a warning to administrators before beginning the process. During the user import process, the health status in the console might report the following warnings on and off: `Driver seems unresponsive | Provisioning | bis_AD_a4uLn | Driver seems unresponsive`.

If you have a large number of users in your environment, ensure that you allow several hours for the provisioning process to complete. After all users have been provisioned, performance of other administration tasks in the console improves considerably.

5 Configuring Social Identity Sources

In addition to using LDAP and JDBC identity sources to authenticate users and provision accounts to SaaS applications, you can configure many social media identity sources in CloudAccess for basic user authentication to SAML applications or web services.

Understanding Social Media Identity Sources in CloudAccess

CloudAccess allows you to configure multiple social media identity sources that customers can use to authenticate to your business' website. These identity sources are identified by an "SSO" designation in the Identity Sources palette on the Admin page of the administration console. CloudAccess creates a SAML assertion using attributes obtained from the identity sources to allow SAML authentications into the resources associated with your website. Customers can log in to CloudAccess using existing social media accounts such as Facebook or LinkedIn and obtain access to specific resources, such as a rewards program, without having to create a new account.

You must configure the identity source and the connector for the identity source for the authentication process to work. In addition, you must map identity source roles (groups) to application authorizations to grant user access to those applications. Policy mapping is an essential step to provide user access. For more information, see Chapter 12, "Mapping Authorizations," on page 91.

Once you have configured the appropriate social identity sources and SAML applications (including appmarks), and mapped identity source roles to application authorizations, users who log in to CloudAccess see the appmarks on the landing page for the applications they are entitled to use.

IMPORTANT: Social media account access is intended to be used only for lightly secured resources, but does not guarantee that identities will be audited and corrected like a corporate directory.

Understanding Linked Logins in CloudAccess

CloudAccess enables users to access resources and applications using social media identities in addition to corporate identities. Social federation in CloudAccess is not created by provisioning; rather, it is user-initiated by linking social accounts to corporate accounts. Linked logins work with any identity source that results in users being provisioned into the local identity vault. You must configure the Linked Logins tool in CloudAccess if you want to enable social federation for your users. For more information, see "Configuring the Connector for Linked Logins" on page 50.

From the end user interface, users have a menu option to link a social identity to their corporate identity. Once they have successfully provided both a social login and user name/password, they are federated and can use either identity to authenticate. This federation does not result in any social attributes other than the social identity's GUID being stored in the CloudAccess identity vault. CloudAccess does not create corporate identities from social identities.

For additional security, you can use a second factor authentication tool such as Advanced Authentication or Fido in conjunction with social federation. When users authenticate using social authentication to an account that is federated, CloudAccess requires them to provide a second factor during authentication. For more information about second factor authentication tools, see Chapter 9, "Configuring Authentication Methods," on page 69.

IMPORTANT: Linked logins offer convenience to users, but they are a potential security breach for organizations. Whenever users access secure corporate resources using a social media account and do not log out, they expose the organization to security risks that CloudAccess cannot control.

Configuring the Connector for Linked Logins

If you want users to be able to access the same resources through CloudAccess with their social media identity as they can with their corporate identity, you must configure the Linked Logins connector tool. Once this tool is enabled, users have the option to link their social media and corporate accounts.

To configure the connector for Linked Logins:

1. Log in with an appliance administrator account to the administration console at

   `https://`*`appliance_dns_name`*`/appliance/index.html`
2. (Optional) If you want to require 2nd factor authentication for social logins, configure the appropriate tool. For more information, see the following:
   - "Configuring the TOTP Tool for Two-Factor Authentication Using Google Authenticator" on page 74
   - "Configuring the Advanced Authentication Tool for Two-Factor Authentication Using the Advanced Authentication Appliance" on page 78
   - "Configuring FIDO for Two-Factor Authentication" on page 80
3. Drag the **Linked Logins** connector from the **Tools** palette to the **Tools** panel.
4. (Conditional) If you configured a 2nd factor authentication tool, click **Require a 2nd factor** and specify which 2nd factor authentication tool you are using.
5. Click **OK**, then click **Apply** to save the configuration.

Configuring Active Directory as an Identity Source

In addition to using Active Directory as an identity source that caches full user accounts and provisions them out to the SaaS applications (Salesforce, Google, ServiceNow, and Office 365), you can configure Active Directory simply to authenticate users so they can access lightly secured resources without actually importing and caching those users. To configure the connector to use Active Directory only as an authentication source, do *not* select the **Enable Local Vault Caching** configuration option.

To configure Active Directory as an identity source for authentication only:

1. Verify that you have an Active Directory administrator account.
2. Log in to the CloudAccess administration console:

   `https://`*`appliance_dns_name`*`/appliance/index.html`

3. Drag the connector for Active Directory from the **Identity Sources** palette to the **Identity Sources** panel.
4. Use the following information to configure the connector for Active Directory:

   Credentials: Specify the fully distinguished LDAP format name and password of the Active Directory administrator account.

   Search Context: Specify the fully distinguished LDAP format of the context where the connector searches for user objects.

   Active Directory Servers: Specify the IP address and LDAP port of the Active Directory server where the user objects reside. Select **Enable LDAP SSL** to use port 636. Otherwise, the default non-SSL port is 389.

   Filter extension: Specify a filter for the object class and attribute you want to use to import users. If users do not meet the criteria defined in the filter, CloudAccess does not import those users.

   For example, `(&(objectclass=user)(samaccountname=abc*))` imports only users that start with the samaccountname of `abc*`.
5. (Optional) If you have custom attributes you want to map, click **Advanced Options**, then specify your custom attributes under **Attribute Mappings**.
6. Click **OK**, then click **Apply** to save the configuration.
7. Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, "Mapping Authorizations," on page 91.

The connector for Active Directory is now an identity source for user logins.

Configuring eDirectory as an Identity Source

In addition to using eDirectory as an identity source that caches full user accounts and provisions them out to the SaaS applications (Salesforce, Google, ServiceNow, and Office 365), you can configure eDirectory simply to authenticate users so they can access lightly secured resources without actually importing and caching those users. To configure the connector to use eDirectory only as an authentication source, do *not* select the **Enable Local Vault Caching** configuration option.

To configure eDirectory as an identity source for authentication only:

1. Verify that you have an eDirectory administrator account.
2. Log in to the CloudAccess administration console:

   ```
   https://appliance_dns_name/appliance/index.html
   ```
3. Drag the connector for eDirectory from the **Identity Sources** palette to the **Identity Sources** panel.
4. Use the following information to configure the connector for eDirectory:

   Credentials: Specify the fully distinguished LDAP format name and password of the eDirectory administrator account with the minimum rights.

   Search Context: Specify the fully distinguished LDAP format of the context where the connector searches for user objects.

   eDirectory Server: Specify the IP address and LDAP port of the eDirectory server that contains a Master or Read/Write replica of the partition where the user objects reside. Select **Enable LDAP SSL** to use port 636. Otherwise, the default non-SSL port is 389.

Filter extension: Specify a filter for the object class and attribute you want to use to import users. If users do not meet the criteria defined in the filter, CloudAccess does not import those users.

For example, `(&(objectclass=user)(samaccountname=abc*))` imports only users that start with the samaccountname of `abc*`.

5 (Optional) If you have custom attributes you want to map, click **Advanced Options**, then specify your custom attributes under **Attribute Mappings**.

6 Click **OK**, then click **Apply** to save the configuration.

7 Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, “Mapping Authorizations,” on page 91.

The connector for eDirectory is now an identity source for user logins.

Configuring reCAPTCHA for Active Directory or eDirectory

You can configure Google reCAPTCHA to work with Active Directory and eDirectory identity sources to provide an additional layer of security for the user login process. For more information about configuring reCAPTCHA, see “Configuring Google reCAPTCHA” on page 70.

Configuring Facebook as an Identity Source

To configure Facebook as an identity source:

1 Install the developer app to your profile from the Facebook Developers (https://developers.facebook.com) website.

2 On the developer site, click **Apps**, then click **Create a New App**.

3 Provide the following information:

- Specify a **Display Name**.
- From the **Category** list, select **Apps for Pages**.

4 Click **Create App**.

5 Click **Settings** in the left pane, then provide the following information:

- In the **App Domains** field, create a new **App Domain** and specify your base DNS name (without `https`) in the format *`appliance_dns_name`*.
- Specify a **Contact Email** address.
- Click **+Add Platform**, then select **Website**.
- Set the value of the **Site URL** field to your CloudAccess appliance publicly resolvable DNS name. For example, `https://`*`appliance_dns_name`*.
- The other fields on this window are not required.
- Click **Save Changes**.

6 Copy the **App ID** value and the **App Secret** value to use when you configure the connector for Facebook.

7 Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

8 Drag the connector for Facebook from the **Identity Sources** palette to the **Identity Sources** panel.

9 Specify the **App ID** and **App Secret** values that you copied from the Facebook configuration.

10 Click **OK**, then click **Apply** to save the configuration.

11 Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, “Mapping Authorizations,” on page 91.

The connector for Facebook is now an identity source for user logins.

Configuring Google as an Identity Source

To configure Google as an identity source:

1 Log in to Google Cloud Console (https://cloud.google.com/console) and create a new project.

2 Open the project you just created, then navigate to **API & Auth** > **Credentials**.

3 Click **Create New Client ID**.

4 Select **Web Application**.

5 Edit the **Authorized Javascript origin** to be the DNS name of your CloudAccess appliance.

6 Edit the **Redirect URI** to include the URL: `https://`*`dns_name`*`/osp/a/t1/auth/oauth2/landingpad`, then change the *dns_name* to the DNS name of your CloudAccess appliance.

7 Click **Create Client ID**.

8 Copy the **Client ID** value and the **Client Secret** value to use when you configure the connector for Google.

9 Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

10 Drag the connector for Google from the **Identity Sources** palette to the **Identity Sources** panel.

11 Use the following information to configure the connector for Google:

Client ID: Specify the **Client ID** value from the Google configuration.

Client Secret: Specify the **Client Secret** value from the Google configuration.

12 Click **OK**, then click **Apply** to save the configuration.

13 Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, “Mapping Authorizations,” on page 91.

The connector for Google is now an identity source for user logins.

Configuring LinkedIn as an Identity Source

To configure LinkedIn as an identity source:

1 Log in to LinkedIn at the LinkedIn Developer website (https://www.linkedin.com/secure/developer).

2 Click **Add New Application**.

3 Create a new application with the following information:

OAuth Accept Redirect URL: Specify `https://`*`dns_name`*`/osp/a/t1/auth/saml2/sso` where the *dns_name* is the DNS name of the CloudAccess appliance.

JavaScript API Domains: Specify `https://`*`dns_name`* where the *dns_name* is the DNS name of the CloudAccess appliance.

4 Copy the API Key value and the Secret Key value to use when you configure the connector for LinkedIn.

5 Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

6 Drag the connector for LinkedIn from the Identity Sources palette to the Identity Sources panel.

7 Use the following information to configure the connector for LinkedIn:

   API Key: Specify the API Key value from the LinkedIn configuration.

   Secret Key: Specify the Secret Key value from the LinkedIn configuration.

8 Click OK, then click Apply to save the configuration.

9 Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, “Mapping Authorizations,” on page 91.

The connector for LinkedIn is now an identity source for user logins.

Configuring MSLive as an Identity Source

To configure MSLive as an identity source:

1 Create an application with a Windows Live login (MS Live) by following the instructions in the MSDN Library Getting Your Client ID for Web Authentication (http://msdn.microsoft.com/en-us/library/bb676626.aspx).

2 Edit the application, then add the DNS name of your CloudAccess appliance as the Target Domain.

3 Under Redirect URIs, add the following URL: `https://`*`<appliance_DNS_name>`*`/osp/a/t1/auth/oauth2/landingpad`.

   NOTE: This URL is required both for new appliance installations and for upgrades from SocialAccess to CloudAccess. If you are upgrading a SocialAccess appliance to CloudAccess, we recommend adding this URL to your existing URLs *before* you upgrade. Otherwise, MSLive authentications will start failing. After you add the URL, however, authentications will succeed again.

4 Copy the Client ID value and the Client Secret value to use when you configure the connector for MSLive in CloudAccess.

5 Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

6 Drag the connector for MSLive from the Identity Sources palette to the Identity Sources panel.

7 Use the following information to configure the connector for MSLive:

   Client ID: Specify the Client ID value from the MSLive configuration.

   Client Secret ID: Specify the Client Secret value from the MSLive configuration.

8 Click OK, then click Apply to save the configuration.

9 Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, “Mapping Authorizations,” on page 91.

The connector for MSLive is now an identity source for user logins.

Configuring Twitter as an Identity Source

To configure Twitter as an identity source:

1. Access the Twitter application at the Twitter Developer website (https://dev.twitter.com/apps).
2. Select **Create a new application**.
3. Create a new application with the following information:

   Website: Specify the publicly resolvable DNS name of your CloudAccess appliance.

   callbackURL: Specify `https://`*`dns_name`*`/osp/a/t1/auth/saml2/sso` where the *dns_name* is the DNS name of the CloudAccess appliance.
4. Copy the **Consumer Key** value and the **Consumer Secret** value to use when you configure the connector for Twitter.
5. Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
6. Drag the connector for Twitter from the **Identity Sources** palette to the **Identity Sources** panel.
7. Use the following information to configure the connector for Twitter:

   Consumer Key: Specify the **Consumer Key** value from the Twitter configuration.

   Consumer Secret: Specify the **Consumer Secret** value from the Twitter configuration.
8. Click **OK**, then click **Apply** to save the configuration.
9. Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, "Mapping Authorizations," on page 91.

The connector for Twitter is now an identity source for user logins.

Configuring Yahoo as an Identity Source

To configure Yahoo as an identity source:

1. Log in to the Yahoo Developer website (https://developer.apps.yahoo.com/).

   You must have a Yahoo developer account to log in to the website.
2. Create a new application with the following information:

   Application Type: Select **Web-based**.

   Home Page URL: Specify `https://`*`dns_name`*`/osp/a/t1/auth/saml2/sso` where the *dns_name* is the DNS name of the CloudAccess appliance.

   Access Scopes: Select **This app requires access to private user data**.

   Callback Domain: Specify `http://`*`dns_name`*, where the *dns_name* is the DNS name for the CloudAccess appliance.

   Permission Scopes: Enable the appropriate **Social Directory (Profiles)** permission as follows:

   - **Read/Write Public and Private** to get *all* attribute values (ID, UserName, FirstName, LastName, BirthDate, Email, Photo, Gender, Language, StreetAddress, City, State, ZipCode, Country, Phone).
   - **Read Public** or **Read/Write Public** to get only the following attribute values: ID, UserName, BirthDate, Photo, Gender, and Language
3. Click **Save and Change Consumer Key**.
4. Click **Verify Domain**, then click **Verify** next to the new domain name.

5. Copy the **Verification filename** value to use when you configure the connector for Yahoo, then click **Verify Domain** again and close the window.
6. Copy the **Consumer Key** and **Consumer Secret** values to use when you configure the connector for Yahoo.
7. Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
8. Drag the connector for Yahoo from the **Identity Sources** palette to the **Identity Sources** panel.
9. Specify the **Consumer Key**, **Consumer Secret**, and **Verification filename** values that you obtained from the Yahoo configuration.
10. Click **OK**, then click **Apply** to save the configuration.
11. Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, "Mapping Authorizations," on page 91.

The connector for Yahoo is now an identity source for user logins.

Configuring OAuth2 Sites as Identity Sources

CloudAccess provides a generic OAuth2 template. The OAuth2 template allows you to configure OAuth2 sites as identity sources for CloudAccess. For more information about OAuth2, see the OAuth2 website (http://oauth.net/2/).

To use the OAuth2 template:

1. Create an OAuth2 application that represents the CloudAccess appliance on the developer site you want to use as an identity source.

   Creating an application does not require any coding.
2. Copy the following information into a document as you create the OAuth2 application to use when configuring the OAuth2 template:
   - Client ID
   - Client Secret ID
   - Authentication URL
   - Token URL or access token
   - Profile URL
   - (Conditional) Profile header
   - Scope separator
3. Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
4. Drag the OAuth2 template from the **Identity Sources** palette to the **Identity Sources** panel.
5. Click the template, then click **Configure**.
6. Use the information gathered in step 2 to create your own connector for OAuth2 following the on-screen prompts.
7. (Optional) You can upload a login card image that is specific to your OAuth2 application in the **Login card image** field. Users see this image when they log in to CloudAccess.

   The image can be a `.png`, `.jpg`, or `.gif` file. The file size is 215px x 50px and the file must be under 1 MB in size.

8 Click **OK**, then click **Apply** to save and create the connector for OAuth2.

9 Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, "Mapping Authorizations," on page 91.

It is common with some OAuth sources for the Token URL or Profile URL to require the oauth_token variable instead of the expected accessToken variable. To fix this, add the following:

```
URL:?oauth_token{$accessToken}
```

For example: `https://api.foursquare.com/v2/users/self?oauth_token={$accessToken}`

Configuring OpenID Connect Sites as Identity Sources

CloudAccess provides a generic OpenID Connect template. The OpenID Connect template allows you to configure OpenID Connect sites as identity sources for CloudAccess. For example, PayPal is an OpenID Connect site.

To use the OpenID Connect template:

1 Create an OpenID Connect application that represents the CloudAccess appliance on the developer site you want to use as an identity source.

Creating an application does not require any coding.

2 Copy the following information into a document as you create the OpenID Connect application to use when configuring the OpenID Connect template:

- (Optional) Discovery URL
- (Optional) Register URL
- Client ID
- Client Secret ID
- Authentication URL
- Token URL
- Profile URL

3 Log in with an appliance administrator account to the CloudAccess administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

4 Drag the OpenID Connect template from the **Identity Sources** palette to the **Identity Sources** panel.

5 Use the information gathered in step 2 to create your own connector for OpenID Connect following the on-screen prompts.

6 (Optional) You can upload a login card image that is specific to your OpenID Connect application in the **Card image** field. Users see this image when they log in to CloudAccess.

The image can be a `.png`, `.jpg`, or `.gif` file. The file size is 215px x 50px and the file must be under 1 MB in size.

7 Click **OK**, then click **Apply** to save and create the connector for OpenID Connect.

8 Proceed to policy mapping to grant users access to applications. For more information, see Chapter 12, "Mapping Authorizations," on page 91.

It is common with some OpenID Connect sources for the Token URL or Profile URL to require the oauth_token variable instead of the expected accessToken variable. To fix this, add the following:

`URL:?oauth_token{$accessToken}`

For example: `https://api.foursquare.com/v2/users/self?oauth_token={$accessToken}`

6 Configuring Self-Service Registration and Password Management

The Self-Service Registration and Password Management tool (SSRPM) allows you to empower users to register for services and to manage their credentials. It provides selected services from the Self-Service Password Reset tool. The Self-Service User Store (SSUS) stores identity and credentials for self-registered user accounts. It is an additional identity source you can use with the appliance.

Enabling a Self-Service User Store

The Self-Service User Store (SSUS) is an internal identity source you can use with the appliance. There are no specific requirements to use this service.

A Self-Service User Store provides self-service registration and password management services. After you enable the service, users can immediately begin to self-register on the SSUS Registration page. Self-registered users can then log in and access public applications from the landing page. Policies are required to allow the self-registered users to access private applications.

NOTE: You can enable and activate only one Self-Service User Store.

By default, SSUS requires new users to have a valid email account to create an SSUS account. Users must be able to receive and respond to a verification email.

You can configure which service options to support for your SSUS users, such as a Help Desk, new user, change password, and forgotten password. You can also enable users to delete their own account.

To enable and configure the SSUS service:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Drag the **Self-Service User Store** icon from the **Identity Sources** palette to the **Identity Sources** panel.
3. On the **Configuration** tab, select the options that you want presented to your users and Help Desk administrators.
4. Click **OK** to enable the Service.
5. Click **Apply** to activate and start SSUS as a service.
6. Wait for the SSUS service to be activated and started across all nodes in the cluster.

   In the **Appliances** panel, the icon on each node of the cluster spins until the service is ready on the node. Do not apply additional changes until this action is complete on all nodes.

   A round green status icon in the lower left corner of the SSUS service icon indicates that the SSUS is configured and its status is healthy.

To allow the self-registered users to access a private application that is enabled for SSUS, continue with "Using SSUS as an Authentication Source for an Application" on page 60.

Using SSUS as an Authentication Source for an Application

The applications are not available for SSUS users until you configure policies that authorize SSUS to be an authentication source for them. All SSUS users receive rights to an application when you assign a policy to the SSUS identity source.

- "Granting SSUS Users Access to a Private Application" on page 60
- "Denying SSUS Users Access to an Application" on page 61

Granting SSUS Users Access to a Private Application

An application can have one or more authorizations for its resources. Each authorization can have one or more appmarks associated with it. (Appmarks are essentially bookmarks for applications. For more information, see "Configuring Appmarks for Connectors" in the *CloudAccess Connectors Guide*.) You grant access to a private application by mapping one or more of its authorizations to the SSUS role. Users can access all of the appmarks associated with an authorization. You cannot control access at the appmark level.

NOTE: You should map authorizations for SSUS roles (groups) only to single sign-on applications. Do not map them to the SaaS applications with account provisioning (Google Apps, Office 365, ServiceNow, or Salesforce). CloudAccess does not support provisioning for users in an SSUS identity source. For more information, see "Requirements for Provisioning" in the *CloudAccess Connectors Guide*.

To create a policy that grants access to an application for SSUS users:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click **Policy** on the toolbar.
3. On the Policy Mapping page, select **Other Identity Sources** from the drop-down list on the left, then select the **All SSUS Users** role.
4. On the right, select the SaaS application that you want to use for this policy, and then view its authorizations.

   Some applications have multiple authorization options.
5. Drag the **All SSUS Users** role from the left side and drop it on the desired authorization on the right.

   You can also select multiple authorizations under a single application, then drag them from the right and drop them on the **All SSUS Users** role on the left.
6. In the Mapping window, review the mapped settings, then click **OK** to accept the new policy, or click **Cancel** to back out of the setup.

   You can remove an authorization in the list by selecting it, then clicking the **Delete** icon.
7. Under **Other Identity Sources**, view the **Authorization** column for the **All SSUS Users** role to confirm that the **Authorization Stamp** icon appears.
8. Under the application on the right, view the **Policy** column to confirm that the **Policy** icon appears for the mapped authorization.

9 The appmarks for each of the mapped authorizations are available to users at their next login.

10 Repeat Step 4 through Step 9 for each application for which you want to use SSUS as an identity source.

Denying SSUS Users Access to an Application

You can deny access to an application by deleting its SSUS policy. Deleting the policy does not interrupt current sessions, but the application is not available to users at their next login.

1 Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

2 Click **Policy** on the toolbar.

3 On the Policy Mapping page, select the **Self-Service User Store** role from the drop-down list on the left, then select the **All SSUS Users** role.

4 In the **All Users** row, click the **Authorization Stamp** icon.

5 In the Edit All Users Mappings window, select the authorization you want to remove, then click **Delete**. Repeat this action for every authorization that you want to remove.

6 Click **OK** to accept the modified settings, or click **Cancel** to back out of the setup.

The application is not available to users at their next login.

Using the Self-Service User Registration and Password Management Services

After you have configured SSUS and mapped policies, users can self-register for accounts and manage their own credentials. Self-registered users can log in to the landing page for the appliance to access applications.

If you enabled the options during the SSUS configuration, users now see links on the appliance login page to create a new account or a link to reset their password if they have forgotten the password.

The user experience is as follows:

1. The new user accesses the appliance login page:

   `https://`*`appliance_dns_name`*

2. The user clicks the link to create a new account.
3. The user follows the on-screen prompts to create a new account that includes their name, email address, and a password.
4. After the account is created, the user is prompted to create security questions and answers.

   If the user forgets the account password, the questions and responses are used to verify the user’s identity and allow the user to reset the password
5. (Conditional) If the user does not create the security questions and answers now, the user will be prompted to create them when they log in for the first time. If the user does not set up the security questions and answers, the appliance will not authenticate the user. The user must set up the security questions and answers to authenticate to the appliance.
6. After the user completes the new account setup, the appliance sends a verification email to the user’s email address. The user responds to verify the account creation.
7. The user accesses the login page again.

8. The user logs in with their new user name and password.
9. The user sees and can access the applications that the policies entitle them to see.

After you enable the Self-Service User Store, the Self-Service User Store login page is available for users. On this page, users can register for the service as a new user, change their password, or reset their forgotten password after answering security questions.

Providing Help Desk Services for Self-Registered Users

The Self-Service User Store (SSUS) provides a Help Desk service. If a password expires or a self-registered user is locked out of an account, an authorized Help Desk user for the SSUS service can reset the password. The Help Desk user sets a temporary randomized password for the account, and the user is notified of the temporary password by email. This allows the user to log in to the account and reset the temporary password to use a custom password.

- "Assigning a User to the Help Desk Role" on page 62
- "Resetting the Password for a Locked Self-Registered User Account" on page 62
- "Deleting a Self-Registered User Account" on page 63

Assigning a User to the Help Desk Role

You must assign a user to the SSUS Help Desk role to provide Help Desk services for the related self-registered users. For more information about assigning roles, see "Assigning Roles to Users" on page 68.

NOTE: You should assign a user from an identity source other than the SSUS source as the Help Desk user.

After you have assigned a user to the SSUS Help Desk role, the Help Desk user can access the Help Desk tools through the CloudAccess landing page.

Resetting the Password for a Locked Self-Registered User Account

An authorized Help Desk user can use the SSUS Help Desk service to reset the password for a self-registered user account. Typically, the user needs Help Desk assistance because the account is locked. If the account is not locked, the user can alternatively reset the password by using the **Forgotten Password** option on the Self-Service Registration login page.

To reset the password for an SSUS account as the authorized Help Desk user:

1. Log in to CloudAccess using your corporate credentials.
2. On the landing page, click the **Help Desk** icon to go to the Help Desk page.
3. On the Help Desk page, search for an SSUS user account, then click the self-registered user's name.
4. On the Password Policy page, view the password policy settings for the user account, then click **Change Password**.
5. On the Account Information page, confirm the user's information, then click **Change Password**.

6. In the **Random Passwords** window, select a password from the list of randomly generated passwords that satisfies the password policy for this account.

   You can click **More** to choose from additional random passwords.

7. View the confirmation message with the new password, then click **OK**.

After the self-registered user receives the temporary password, the user is prompted to reset the password at their next login.

Deleting a Self-Registered User Account

An authorized Help Desk user can use the SSUS Help Desk service to delete the SSUS account for a self-registered user.

To delete an SSUS account as the authorized Help Desk user:

1. Log in to CloudAccess using your corporate credentials.
2. On the landing page, click the **Help Desk** icon to go to the Help Desk page.
3. On the Help Desk page, search for the SSUS user whose account you want to delete, then click the self-registered user’s name.
4. On the Account Information page, confirm the user’s information, then click **Delete Account**.
5. Click **OK** to confirm the account deletion.

7 Configuring SAML 2.0 Inbound Identity Sources

You can create a custom connector that allows users to authenticate to the CloudAccess appliance through a SAML federated connection. To create this federation, you must create a custom SAML In connector.

To allow the appliance to be a SAML 2.0 service provider, you can create a SAML 2.0 Inbound connector using the Access Connector Toolkit. After you export the connector and import it in the appliance, the SAML2 In connector appears as an identity source. You configure an instance of the identity source with information about an appropriate identity provider to enable the service provider functionality of the appliance, and to allow the identity provider to send a SAML token to the appliance using the SAML 2.0 POST profile.

After you configure the SAML2 In identity source, the appliance login page provides a link to the login page of the SAML 2.0 identity provider, located to the left of the user name and password login options. The SAML 2.0 users log in through the identity provider to gain access to the appliance landing page.

For more information, see "Creating a SAML 2.0 Inbound (SAML2 In) Connector Template" in the *CloudAccess Connectors Guide*.

8 Configuring Roles Management

CloudAccess provides the ability to assign different roles to administrative users in your identity sources. The roles allow administrators to perform certain tasks and deny them access to other tasks.

Understanding CloudAccess Role Types

CloudAccess includes the following types of roles:

- **Appliance Administrator:** One or more users can have the appliance administrator role in CloudAccess. CloudAccess has a default administrator account (appliance.admin) that you use to log in to the appliance for the first time after initializing the appliance.

  The default appliance administrator has rights to access the Admin, Roles, Policy, Reports, and Devices pages. This administrator has rights to add and remove identity sources, tools, nodes, and applications. However, this administrator does not have application ownership and approval rights by default.

  When an appliance administrator assigns a user the appliance administrator role, the new administrator also has rights to access the Admin, Roles, Policy, Reports, and Devices pages. However, like the first appliance administrator, subsequent administrators do not have application ownership and approval rights by default.

  Only appliance administrators can add SaaS applications, such as Google Apps and Salesforce. Any appliance administrator that imports and applies a SaaS application is also made that application owner and has rights to the Approvals page for that specific application. An appliance administrator who is also an application owner can assign another administrator to be the application owner and application approver, and can either keep or remove himself from those roles.
- **Application Owner:** The application owner controls access to the SaaS applications. CloudAccess automatically assigns this role to the user who creates the SaaS application on the Admin page. The application owner can access the following web pages:
  - **Approvals:** The application owner can allow or deny approvals for users to obtain a SaaS application account.
  - **Policy:** The application owner can map authorizations between the identity source and the SaaS application and optionally require approval for authorizations.
  - **Roles:** The application owner can add or remove users from the application approver role.
- **Application Approver:** The application approver can access the Approvals page and allow or deny approvals for users to obtain a SaaS application account. CloudAccess automatically assigns this role to the administrator who creates the SaaS application on the Admin page.
- **Compliance Auditor:** The compliance auditor can access the Reports page and generate, view, and download the reports for the appliance. Users assigned to the appliance administrator role automatically have access to the Reports page.
- **Device Administrator:** The device administrator can view and delete other users' registered mobile devices on the Devices page. Users assigned to the appliance administrator role automatically have the device administrator role (though device administrators do not automatically have the appliance administrator role).

- **Help Desk:** The Help Desk administrator manages the Self-Service User Store users. The Help Desk user can delete users and reset passwords.

In addition to the default role assignments, you can assign each role to additional users. However, the Roles page never allows you to remove the last appliance administrator role.

Assigning Roles to Users

To assign roles to users:

1. Log in to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html` as the appliance administrator or application owner.
2. Click **Roles** on the toolbar.
3. Type the name of a user into the search filter field, then click **Search**. Matching users appear in the left column.

   NOTE: This is not a regular expression filter. An asterisk (*) is the only wildcard character allowed. CloudAccess modifies the filter to include (*) on the front and end of whatever you type. For example, a filter for "`test`" would end up as the LDAP filter expression "`*test*`".

4. Drag the user name from the left side and drop it on the role that you want to assign to that user on the right side.
5. In the Add User to Role window, review the mapped settings, then click **OK** to accept the new role assignment.
6. After the page refreshes, view the **Role** column for the user to confirm that the **Role** icon appears, and verify that the authorized user’s name appears under the Help Desk role on the right.

The Roles page displays only the application owner and application approver roles of configured SaaS connectors.

9 Configuring Authentication Methods

The CloudAccess appliance allows you to configure one or more authentication methods for users. Some of the authentication methods are additive. For example, you can use Google reCAPTCHA with Integrated Windows Authentication. Use the information in the following sections to configure authentication methods for the appliance.

Configuring Integrated Windows Authentication with Kerberos

CloudAccess allows user authentication with either name and password or Integrated Windows Authentication with Kerberos if your identity source is Active Directory. If you choose to use Integrated Windows Authentication, you must configure Kerberos.

CloudAccess supports the use of only one Kerberos realm. If there are multiple Active Directory domains used as the identity source, all of the domains must use the same realm.

Use the information in the following sections to enable Kerberos authentication between Active Directory and CloudAccess.

- "Configuring the Kerberos User in Active Directory" on page 69
- "Configuring the Appliance to Use Integrated Windows Authentication with Kerberos" on page 70
- "Configuring User Browsers" on page 70

Configuring the Kerberos User in Active Directory

To configure Kerberos in your Active Directory domain:

1 As an Administrator in Active Directory, use the Microsoft Management Console (MMC) to create a new user within the search context specified during the initialization of the appliance.

Name the new user according to the Host and DNS name of the appliance. For example, if the public DNS of the appliance is serv1.mydomain.com, the context that has been enabled for cloud is ou=acme corporation,dc=mydomain,dc=com, and the AD domain is EXAMPLE.COM, use the following information to create the user:

First name: serv1

User login name: HTTP/serv1.mydomain.com

Pre-windows logon name: serv1

Set password: Specify the desired password. For example: Passw0rd

Password never expires: Select this option.

2 Associate the new user with the service principal name.

Any domain or realm references must be uppercase.

2a On the Active Directory server, open a cmd shell.

2b At the command prompt, enter the following:

```
setspn -A HTTP/appliancepublicdns@UPN.SUFFIX newusershortname
```

For example: `setspn -A HTTP/serv1.mydomain.com@EXAMPLE.COM serv1`

2c Verify setspn by entering `setspn -L` *`shortusername`*

For example: `setspn -L serv1`

3 Generate the `keytab` file using the `ktpass` utility.

Any domain or realm references must be uppercase.

3a At the command prompt, enter the following:

```
ktpass /out filename /princ servicePrincipalName /mapuser userPrincipalName
/pass userPassword
```

For example: `ktpass /out nidp.keytab /princ HTTP/serv1.mydomain.com@EXAMPLE.COM /mapuser serv1@EXAMPLE.COM /pass Passw0rd`

3b Ignore the message `Warning: pType and account type do not match`.

4 Copy the `nidp.keytab` file created in Step 3 to the browser of the client computer that you are using for CloudAccess administration.

Configuring the Appliance to Use Integrated Windows Authentication with Kerberos

The following steps enable the CloudAccess appliance to use Integrated Windows Authentication (IWA) with Kerberos, if your identity source is Active Directory.

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. On the **Tools** panel, click the **Integrated Windows Authentication** icon, then click **Configure**.

   NOTE: The IWA options are global for all connectors for Active Directory. You configure the IWA options only once, regardless of the number of connectors for Active Directory you have configured.

3. Next to the **Keytab** field click **Choose Files**, then browse to and select the `nidp.keytab` file generated in "Configuring the Kerberos User in Active Directory" on page 69.
4. Click **OK** to save the changes.
5. Click **Apply** to apply the changes to the appliance.

Configuring User Browsers

To complete the Kerberos configuration for Active Directory, configure the user browser. For more information, see "Configuring End User Browsers for Kerberos Authentication" on page 100.

Configuring Google reCAPTCHA

The Google reCAPTCHA tool helps protect your user login page against spam, malicious registrations, and other forms of attack where computers disguise themselves as humans. It provides an additional layer of security by displaying images of words that users must type in addition to their login credentials. Software bots typically cannot scan the images to provide a response.

Using reCAPTCHA helps prevent automated Denial of Service (DoS) attacks that can impact the performance of the appliance and the identity source. The tool uses the remote Google reCAPTCHA service to provide the images and verify the responses. If a response succeeds, the appliance verifies the user’s authentication credentials against the identity source. If a response fails, the appliance fails the login attempt without processing the credentials, and re-displays the login page. Thus, the automated login attempts fail and cannot consume the processing resources of the appliance and identity source.

Use the information in the following sections to configure your system for reCAPTCHA:

- “Requirements for reCAPTCHA” on page 71
- “Configuring Intrusion Detection for Failed Logins” on page 71
- “Configuring a Google reCAPTCHA Account” on page 72
- “Configuring the reCAPTCHA Tool” on page 73

Requirements for reCAPTCHA

Ensure that your system meets the following requirements before you configure the Google reCAPTCHA tool:

- ❒ A CloudAccess appliance, installed and configured.
- ❒ One or more supported identity sources, with the connectors enabled and configured.

  The reCAPTCHA tool supports users from Active Directory, eDirectory, and Self-Service User Store (SSUS) identity sources. It does not support users from other types of identity sources, such as users imported from Microsoft SQL Server or Oracle Database type identity sources that use the JDBC identity source connector.

  Each identity source should be configured with an intrusion detection policy. For more information, see “Configuring Intrusion Detection for Failed Logins” on page 71.
- ❒ A Google reCAPTCHA account, configured on the Google reCAPTCHA website. For more information, see “Configuring a Google reCAPTCHA Account” on page 72.

Configuring Intrusion Detection for Failed Logins

Someone who attempts to use more than a few unsuccessful passwords while trying to log on to your system might be a malicious user. reCAPTCHA cannot prevent attacks by anyone who can read the image. It cannot differentiate between malicious users and legitimate users. Using reCAPTCHA cannot prevent coordinated human DoS attacks. If users have unlimited attempts to enter their authentication credentials, reCAPTCHA also cannot help prevent attacks to find passwords.

To help limit the effectiveness of brute force or human attacks that bypass the reCAPTCHA protection, you should enable the user’s identity source to respond to this type of potential attack by disabling the account for a preset period of time after a specified number of failed logon attempts.

The supported identity sources have the following built-in intrusion detection systems:

- **Active Directory Account Lockout Policy:** Active Directory allows you to specify an account lockout policy for users and global security groups in a domain. Set the policy on the domain group policy object from the domain controller.

  To configure the Account Lockout Policy settings:

  1. Log in as an Active Directory administrator user to the Windows Server that hosts Active Directory Domain Services (the domain controller).
  2. Configure the Account Lockout Policy on the group policy object for the domain controller.

For more information, see the *Account Lockout Policy* (http://technet.microsoft.com/en-us/library/hh994563%28v=ws.10%29.aspx) in the Microsoft TechNet Library. (http://technet.microsoft.com/)

3. Verify that the **Account Lockout Threshold** value is higher than the number of failed login attempts you plan to specify for **Start reCAPTCHA at** in the reCAPTCHA tool.
4. Repeat these steps for each configured Active Directory identity source.

- **eDirectory Intruder Lockout Policy:** eDirectory allows you to enable Intruder Detection and specify an Intruder Lockout policy for the container object where your user objects reside.

  To configure the eDirectory Intruder Detection and Intruder Lockout Policy:

  1. Log in as the eDirectory administrator user to the management console for the eDirectory server.
  2. Configure Intruder Detection and the Intruder Lockout policy on the container object where your user objects reside.

     For more information, see "Setting Up Intruder Detection for All Users in a Container" (https://www.netiq.com/documentation/edir88/edir88/data/afxkmdi.html#a3p5g0i) in the *eDirectory 8.8 SP8 Administration Guide*.
  3. Verify that the Intruder Lockout value is higher than the number of failed login attempts you plan to specify for **Start reCAPTCHA at** in the reCAPTCHA tool.
  4. Repeat these steps for each configured eDirectory identity source.

- **SSUS Lock Account After Detection:** The SSUS identity store automatically enables the Lock Account After Detection option. It allows up to 7 consecutive failed login attempts within a 30-minute interval. If the next login attempt also fails within the interval, SSUS locks the account for 15 minutes. After 15 minutes, the system automatically unlocks the account, and the user can log in using a correct user name and password. To log in before the lockout is reset, the user can contact the SSUS Help Desk and ask the administrator to reset the password.

After you have configured intrusion detection for the supported identity sources, continue with "Configuring a Google reCAPTCHA Account" on page 72.

Configuring a Google reCAPTCHA Account

Before you configure the Google reCAPTCHA tool, you must configure an account to use for your domain at Google reCAPTCHA, and create a public and private key.

To configure a Google reCAPTCHA account to use for your appliance's domain:

1. Access the Google reCAPTCHA (https://www.google.com/recaptcha/) website.
2. Click **Get reCAPTCHA > Sign up Now**.
3. Log in using one of your Google accounts.

   For example, if you use your Gmail account, the reCAPTCHA account is associated with the Gmail account.
4. (Conditional) If this is not your first site, click **Add a New Site**. Otherwise, skip to the next step.
5. Specify a domain.

   Read the **Tips** for more information.
6. Click **Create** to add the domain.
7. Copy the **Public Key** and **Private Key** that the interface displays to use when you configure the identity source.
8. Continue with "Configuring the reCAPTCHA Tool" on page 73.

Configuring the reCAPTCHA Tool

Before you configure the Google reCAPTCHA tool, you must set up intruder detection in the Active Directory and eDirectory identity sources, and create public and private keys for your appliance's domain at the Google reCAPTCHA website.

To configure the reCAPTCHA service:

1. Using the identity source's native management tools, verify that its intrusion detection setup meets the requirements specified in "Configuring Intrusion Detection for Failed Logins" on page 71.
2. Log in with an appliance administrator account to the administration console at

   `https://`*`appliance_dns_name`*`/appliance/index.html`
3. In the **Identity Sources** panel, verify that you have configured an identity source for Active Directory or eDirectory, or both.
4. Drag the **reCAPTCHA** tool from the **Tools** palette to the **Tools** panel.
5. Configure the reCAPTCHA feature as follows:

   Start reCAPTCHA at: Specify how many failed login attempts must occur before the login page displays the reCAPTCHA prompt. The value should be less than the lockout value set in the identity sources' intrusion detection system.

   - If the reCAPTCHA count is set to zero, the login page displays a reCAPTCHA prompt every time for all users. Every login requires user credentials and the reCAPTCHA response.
   - If the reCAPTCHA count is greater than zero, the login page displays the reCAPTCHA prompt only after the user login fails the specified number of times in the same browser window.

   Public Key: Paste the Public Key value from your reCAPTCHA account configuration for this appliance's domain.

   Private Key: Paste the Private Key value from your reCAPTCHA account configuration for this appliance's domain.

   For information about the public and private keys for your reCAPTCHA account, see "Configuring a Google reCAPTCHA Account" on page 72.
6. Click **OK** to save the settings and enable the tool.
7. Click **Apply** to activate the configuration.
8. Wait while the service is activated across all nodes in the cluster. Do not attempt other configuration actions until the activation completes successfully.

Configuring the TOTP Tool for Two-Factor Authentication Using Google Authenticator

The Time-Based One-Time Password (TOTP) tool in CloudAccess supports the use of one-time passwords (OTPs) for two-factor authentication of users as they access applications through CloudAccess. With two-factor authentication, users must provide two categories of authentication factors before they can access the applications. The authentication factors used by the TOTP tool are:

- **Something the user knows:** The first authentication factor requires *something the user knows*, such as the password for the user's single-sign-on user name.
- **Something the user has:** The second authentication factor requires *something the user has*, such as a mobile device running Google Authenticator to generate time-based one-time passwords.

  Google Authenticator is a free software-token app that users deploy on their mobile devices. Authenticator generates time-based OTPs for authentication, without requiring an Internet connection or cellular service.

If users construct strong passwords and protect them, one-factor authentication can be an effective measure against security breaches. Two-factor authentication provides an additional layer of security to help ensure the identity of a user and reduce the risk of unauthorized access to your applications and data. Users still enjoy the convenience of single sign-on, but the access is more secure.

The following sections describe how to set up and use TOTP for CloudAccess:

- "Configuring the TOTP Tool" on page 74
- "Registering a Mobile Device with the TOTP Tool for OTP Generation" on page 75
- "Using Two-Factor Authentication at Login" on page 77
- "Resetting a Device (Unregistering a Device)" on page 77

Configuring the TOTP Tool

You can enable the Time-Based One-Time Password tool to require users to use two-factor authentication when logging in through CloudAccess.

To configure the TOTP tool:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Drag the **TOTP Tool** icon from the **Tools** palette to the **Tools** panel.
3. Click the **TOTP** icon on the **Tools** panel, then click **Configure**.
4. (Optional) Specify the **Validity Time**.

   Specify an integer value from 2 to 10. The default value is 5. Shorter validity times are considered more secure.
5. Click the **Applications** tab, then select the check box next to one or more applications to enable them for TOTP.

   By default, no applications are enabled for TOTP.

   When a user registers an authentication device, the device and authentication codes apply to all TOTP-enabled applications.
6. Click **OK** to save the setting and enable the TOTP tool.

7 Click **Apply** to activate the TOTP configuration.

8 Wait while the service is activated across all nodes in the cluster. Do not attempt other configuration actions until the activation completes successfully.

In the Appliances pane, a green gear icon spins on top of each node until the activation is complete across all nodes in the cluster.

Registering a Mobile Device with the TOTP Tool for OTP Generation

After you enable the TOTP tool, users are prompted to register a device to use for the additional verification the next time they sign in to CloudAccess. Each user must register a mobile device for generating the user’s one-time passwords. For the initial setup, the user should use a web browser on a computer other than the mobile device where the one-time passwords will be generated.

The One-Time Authentication code page displays a QR code and its equivalent secret key. The user deploys the Google Authenticator app on a mobile device, and sets up an account for CloudAccess by using the shared key. The user can scan the QR code or manually enter the key. When the app runs, it generates a new one-time password every 30 seconds.

Before registering a device, the following setup is required:

❒ The user must be an authorized user of CloudAccess with a valid user name and password.

❒ The user must have access to a computer running a supported web browser.

For a list of supported web browsers, see Table 2-2, “Product Requirements,” on page 18.

❒ The user must use a supported mobile device.

For a list of supported mobile device platforms, see Table 2-2, “Product Requirements,” on page 18.

❒ The user must install the Google Authenticator app on the mobile device.

To register a mobile device for use with the TOTP tool:

1 (Conditional) If the Google Authenticator mobile app is not already installed on the mobile device, download and install it.

1a Visit the app store for your mobile device.

1b Search for Google Authenticator.

1c Download and install the app.

2 From a computer that will not be used as the OTP device, access CloudAccess either directly or through a SAML2 redirect.

3 On the CloudAccess login page, enter your network user name and password (your normal identity source login credentials).

A message displays a QR code (and its equivalent secret key) to use for the TOTP registration.

If you are not prepared to register your mobile device at this time, you can cancel the registration process by closing the tab or your browser. On your next login, CloudAccess generates a new secret key, and prompts you to register a device with a new key.

4 On your mobile device, use the Google Authenticator app to scan the displayed QR code, and register the device with CloudAccess. You can alternatively type the secret key.

4a On your mobile device, open the Google Authenticator app.

4b Select **Settings** > **Add an account**.

4c Use either of the following methods to configure the account:

- **Scan a barcode:**
  1. Select **Scan a barcode**.
  2. Use your device's camera to scan the QR code that appears on the CloudAccess One-Time Authentication Code page.
- **Enter provided key:**
  1. Select **Time Based**.
  2. Select **Enter provided key**.
  3. Type the 16-character secret key that appears on the CloudAccess One-Time Authentication Code page. The key is case sensitive. Do not add spaces or stray characters.

4d Specify a unique name for the account.

4e Tap **Done**.

5 On the mobile device, view the 6-character code that Google Authenticator displays for CloudAccess. This is your OTP.

6 On the computer on the One-Time Authentication Code page, type the OTP, then click **Sign In**.

CloudAccess confirms that the mobile device is registered, and the login is successful.

If the code does not validate, the registration page is redisplayed with the current secret key. You can generate a new code, and try again. The code might not validate if you enter an expired code, you do not enter a code, you mistype the code, or you make an error when setting up the secret key for the account in Google Authenticator.

7 To log in to your account from the mobile device, log in to CloudAccess as described in "Using Two-Factor Authentication at Login" on page 77.

On successful authentication, you can access the apps icons for the authorized services and resources associated with your user identity. Access is granted only for the duration of that session.

To deregister a mobile device:

1 Access CloudAccess, either directly or through a SAML2 redirect.

2 Log in and authenticate as described in "Using Two-Factor Authentication at Login" on page 77.

3 Click the **My Devices** icon.

4 In the **Registered Devices** list, select the mobile device.

5 Click the **Delete** icon for the device.

6 In the **Unregister** Device window, click OK to confirm.

At your next login, CloudAccess prompts you to register a device before you can access applications that require two-factor authentication.

Using Two-Factor Authentication at Login

When two-factor authentication is enabled for CloudAccess, a user must provide login credentials and a one-time authentication code to gain access to TOTP-enabled applications. The code is a 6-digit number generated for CloudAccess by the Google Authenticator app that is running on the user's mobile device. The user must have already registered the mobile device with CloudAccess, as described in "Registering a Mobile Device with the TOTP Tool for OTP Generation" on page 75.

The user should enter the newly generated code as soon as possible after it appears in the Google Authenticator app. Each OTP is intended for use by only one user, is valid for 30 seconds, and becomes invalid after the user successfully logs in. Access is granted only for the duration of that session.

To log in to CloudAccess using two-factor authentication:

1. Access CloudAccess, either directly or through a SAML2 redirect.
2. On the login page, enter your network user name and password (your normal identity source login credentials).

   CloudAccess verifies the credentials against a defined identity source. If all applications require two-factor authentication, the One-Time Authentication Code page appears and prompts you to enter the code. Otherwise, CloudAccess displays the page when you first click any one of the applications that require it.
3. Use Google Authenticator to generate a new one-time password, and enter the code on the CloudAccess One-Time Authentication Code page.

   If you enter the password incorrectly, you can try again with the same password until it times out. Google Authenticator generates a new OTP every 30 seconds.

   On successful authentication, you can access the apps icons for the authorized services and resources associated with your user identity. Each session requires only a single successful authentication.

Resetting a Device (Unregistering a Device)

Each user can register a single device to use for generating one-time passwords. Resetting a device for a user's account unregisters the user's current device. The next time the user logs in, the TOTP tool creates a new secret key for the account.

An administrator can reset a device for a user account:

- To allow the user to register a different device
- To revoke access for a registered device that is lost or stolen

Information about a user's registered device and secret key is part of the user's identity information in the identity source. This information is deleted automatically if a user's identity object is permanently deleted from the identity source. The information is stored with the user's object if the user's identity object is disabled.

If the Time-Based One-Time Password tool is disabled, CloudAccess no longer prompts the users for an OTP at login. However, information about a user's registered device and secret key continue to be stored in the users' identity objects in the identity source. The OTPs generated for the user's CloudAccess account by the Google Authenticator app are no longer needed at login.

After a device is unregistered, the OTPs generated for the user's CloudAccess account by the Google Authenticator app are no longer valid. At the user's next login, the TOTP tool generates a new secret key for the user, and the user must register a device to work with it.

Users can reset a device for their own account, and do not need administrator approval or permission to reset a Google TOTP registration. However, administrators can also reset or unregister devices for other users as needed.

To reset (unregister) a device for your own account:

1. Log in with your appliance user name and password.
2. Click your name in the top right corner to display the drop-down menu.
3. Click **Reset One Time Password**.
4. Click **Yes** to confirm that you want to reset your TOTP password.

To reset (unregister) a device for a user account as an administrator user:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click the **Devices** icon.
3. In the **User** field, type in the user name of the account for which you need to reset TOTP.
4. Click **Reset One Time Password for *First-name Last-name***.

Configuring the Advanced Authentication Tool for Two-Factor Authentication Using the Advanced Authentication Appliance

The Advanced Authentication tool in CloudAccess supports the use of one-time passwords (OTPs) for two-factor authentication of users as they access applications through CloudAccess. The tool works with the Advanced Authentication appliance.

With two-factor authentication, users must provide two categories of authentication factors before they can access the applications:

- **Something the user knows:** The first authentication factor requires *something the user knows*, such as the password for the user’s single-sign-on user name.
- **Something the user has:** The second authentication factor requires *something the user has*, such as a device to uniquely generate or receive one-time passwords or authentication requests that can be used only for that access moment.

Two-factor authentication provides an additional layer of security that helps ensure the identity of a user and reduce the risk of unauthorized access to your applications. Users still enjoy the convenience of single sign-on, but the access is more secure.

The Advanced Authentication tool in CloudAccess supports multiple types of authentication providers for OTP in the Advanced Authentication appliance. You configure a separate instance of the tool for each authentication provider type you want users to use. For each authentication provider type, you can enable one or more applications, but they must be mutually exclusive of the applications that you enable in other instances. The applications must also be mutually exclusive of applications configured to use the Time-Based One-Time Password tool with Google Authenticator.

At a user’s next login, the tool prompts the user for additional authentication, according to the authentication provider type enabled for the application. If you enable a single authentication provider type for all applications, the prompt occurs immediately after CloudAccess validates the user’s credentials. Otherwise, the prompt occurs when the user first selects any one of the applications enabled for Advanced Authentication. The authentication automatically applies to all applications for that session that were also enabled for the same type of authentication provider.

For more information about using the Advanced Authentication appliance and the supported authentication providers, see the Advanced Authentication (https://www.netiq.com/documentation/advanced-authentication-framework/) documentation website.

Use the information in the following sections to configure your system for Advanced Authentication:

- "Requirements for Advanced Authentication" on page 79
- "Configuring the Advanced Authentication Tool" on page 79

Requirements for Advanced Authentication

Ensure that your system meets the following requirements before you configure Advanced Authentication as an authentication method:

- □ A CloudAccess appliance, installed and configured.
- □ An Advanced Authentication 5.*x* or later appliance, installed and configured.
- □ The Advanced Authentication tool in CloudAccess supports many of the authentication providers available in Advanced Authentication.

  Before you configure the Advanced Authentication tool, ensure that you install and configure the authentication providers that you want to use on the Advanced Authentication appliance. For more information, see the Advanced Authentication (https://www.netiq.com/documentation/advanced-authentication-framework/) documentation website.

  For SMS and Voice Call, the user's telephone number that will be used for authentication should be specified in the user's properties in Active Directory.
- □ The users must use the Advanced Authentication client or web user interface to enroll or re-enroll for the authentication providers that you want them to use.
- □ Identify the type of authentication provider that you want to use for each of your destination applications.

NOTE: You can use the Advanced Authentication appliance for applications on desktop browsers, but this does not work on mobile devices. When users access an application from the MobileAccess app, they are automatically logged in, ignoring any advanced authentication rules that you configure in CloudAccess. The MobileAccess app supports only OAuth by design.

Configuring the Advanced Authentication Tool

Before you configure the Advanced Authentication tool, ensure that your setup meets the requirements described in "Requirements for Advanced Authentication" on page 79.

To configure the Advanced Authentication tool:

1. Log in with an appliance administrator account to the administration console at

   `https://`*`appliance_dns_name`*`/appliance/index.html`
2. Drag the **Advanced Authentication** tool from the **Tools** palette to the **Tools** panel.
3. Configure the Advanced Authentication feature:

   Authentication type: Select the type of authentication provider that you want to enable for the specified Advanced Authentication appliance.

   NAAF host name/port: Specify the host name of the Advanced Authentication appliance. The default port number is 443.

4. Click the **Applications** tab, then select the check box next to one or more applications that require the specification authentication provider.

   You can enable one or more applications for the specified type of authentication provider. However, you must assign each application to only one type of authentication provider.
5. Click **OK** to save the settings and enable the tool.
6. Click **Apply** to activate the configuration.
7. Wait while the service is activated across all nodes in the cluster. Do not attempt other configuration actions until the activation completes successfully.

Configuring FIDO for Two-Factor Authentication

CloudAccess supports FIDO (Fast IDentity Online) for two-factor authentication. FIDO requires that users enter their user name and password. The second factor authentication is a dongle that users must touch to authenticate. For more information, see the FIDO Alliance (https://fidoalliance.org/) website.

Requirements for FIDO

Ensure that your system meets the following requirements before you configure FIDO as an authentication method:

❐ A CloudAccess appliance, installed and configured.

❐ A FIDO supported dongle for each user.

NOTE: End users must use a Chrome browser to register their YubiKey device.

Configuring the FIDO Tool

Before you configure the FIDO tool, ensure that your setup meets the requirements described in “Requirements for FIDO” on page 80.

To configure the FIDO tool:

1. Log in with an appliance administrator account to the administration console at

   `https://`*`appliance_dns_name`*`/appliance/index.html`
2. Drag the **FIDO** tool from the **Tools** palette to the **Tools** panel.
3. Read the message that there is no configuration required.
4. Click the **Applications** tab, then select the check box next to one or more applications that require the specified authentication provider.

   You can enable one or more applications for the specified type of authentication provider. However, you must assign each application to only one type of authentication provider.
5. Click **OK** to save the settings and enable the tool.
6. Click **Apply** to activate the configuration.
7. Wait while the service is activated across all nodes in the cluster. Do not attempt other configuration actions until the activation completes successfully.

Resetting (Unregistering) a FIDO Device

Users can reset a device for their own account, and do not need administrator approval or permission to reset a FIDO registration. However, administrators can also reset or unregister devices for other users as needed.

To reset (unregister) a device for your own account:

1. Log in with your appliance user name and password.
2. Click your name in the top right corner to display the drop-down menu.
3. Click **Unregister FIDO Device**.
4. Click **Yes** to confirm that you want to reset your FIDO device.

To reset (unregister) a device for a user account as an administrator user:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click the **Devices** icon.
3. In the **User** field, type in the user name of the account for which you need to reset the FIDO device.
4. Click **Unregister FIDO Device for *First-name Last-name***.

10 Configuring Mobile Access for Users

Administrators can enable user access to SSO, proxy, and SaaS applications from supported mobile devices. For more information about supported mobile devices, see "Product Requirements" on page 18.

Introduction to Mobile Access

Mobile access features are available for all application connectors that CloudAccess supports. Configurable mobile access options include the following:

- Which applications users should be able to access.
- Whether users can access an application through a desktop browser or a mobile device, or both.
- The preferred viewer for the application on the mobile device.
- Whether users are required to provide a PIN to use the MobileAccess app on their mobile devices, and if so, whether they are required to re-enter the PIN after a period of inactivity.

The MobileAccess app that end users install on their mobile devices enables them to access corporate and SaaS applications from those devices. Administrators can also make the MobileAccess app available to users in a private corporate store. After users have installed the app and registered their device, they can access assigned applications using their corporate user name and password.

NOTE: The MobileAccess app is HTTPS-only, and does not work over an unsecured connection.

Administrators can unregister user mobile devices in the administration console. So, if a registered mobile device is lost or stolen, or an employee leaves the company, you can ensure that unauthorized users cannot access corporate resources. Users can also unregister their own mobile devices if necessary, either from their device or from the appliance administration console.

Configuring the Mobile Tool on the Appliance

After you have installed and configured the appliance, you must configure the Mobile tool if you want to provide mobile access for users.

To configure the Mobile tool:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Drag the **Mobile** icon from the **Tools** palette to the **Tools** panel.
3. Click the **Mobile** icon on the **Tools** panel and then click **Configure**.
4. In the **Display name** field on the Mobile Application Access window, type your company name. This name appears in the bar at the top of the MobileAccess app window on users' mobile devices.

5. In the **Prompt for Password Re-authentication in x Days** field, specify how long users can continue to use an authenticated password on mobile devices before re-authentication is required.
6. (Optional) On the **Ask for pin** bar, specify whether users must set a PIN for the MobileAccess app on their mobile devices, and whether they must re-enter the PIN after a period of inactivity. You can change this requirement at any time. For more information, see "Understanding the MobileAccess PIN" on page 87.
7. Click **OK**.
8. Click **Apply** on the Admin page.
9. Wait for the apply operation to finish. (The gear stops spinning on the appliance when the operation has finished.)
10. Continue with "Replacing the Default Certificate on the Appliance" on page 84.

Replacing the Default Certificate on the Appliance

You must change the default certificate that comes with the appliance before you can successfully register mobile devices. For security reasons that are well-documented, as well as for administrator and user convenience, we highly recommend that you change the default certificate on the appliance to a well-known Certificate Authority signed certificate. For more information, see "Changing the Certificates on the Appliance" on page 29.

Before you change the certificate on the appliance, ensure that your environment meets the following requirements:

- ❒ The appliance must be installed and running with a DNS entry that points to it.
- ❒ The certificate must be at least 2K key size (4K preferably) using SHA256.
- ❒ The certificate must be signed by a Certificate Authority, preferably a well-known Certificate Authority. If you choose to use a self-signed certificate, it must be flagged as a certificate authority.

If you use a self-signed or non-public CA-signed certificate, users must also install the certificate on their mobile devices. For more information, see the following topics:

- "Generating a Self-Signed Certificate" on page 84
- "Installing a Self-Signed Certificate on the Mobile Device" on page 85

Generating a Self-Signed Certificate

You can generate a self-signed certificate and use it on the appliance, but if you do so, you must also perform the steps in "Installing a Self-Signed Certificate on the Mobile Device" on page 85 to ensure that you can successfully register mobile devices. You can run the Java 7 keytool on a computer other than the appliance to generate the certificate.

To generate a self-signed certificate:

1. Using the Java 7 keytool, use the following commands replacing *name* and *appliance_dns_name*:

```
keytool -genkeypair -keystore name.p12 -storepass changeit -sigalg
SHA256withRSA -keyalg RSA -keysize 4096 -dname "CN=appliance_dns_name" -
validity 365 -storetype pkcs12 -ext bc=ca:true
```

name can be anything you want, as long as it is the same between the two commands, and you can find it when you want to upload it.

appliance_dns_name must be the DNS name of the appliance.

The output of this command is a `.p12` format file. You can use this file to replace the default certificate on the appliance. (Use the password of `changeit` when the administration console prompts for it.) For more information, see "Changing the Certificates on the Appliance" on page 29.

2. To get the public certificate from that keyfile (which you will use when you perform the procedure in "Installing a Self-Signed Certificate on the Mobile Device" on page 85), use the following command, replacing *name* with the same value from above:

```
keytool -export -keystore name.p12 -storetype pkcs12 -alias mykey -file
name.cer -storepass changeit
```

   The output of this command is a `name.cer` file that you can use later.

Installing a Self-Signed Certificate on the Mobile Device

This procedure is required only if you used the commands in "Replacing the Default Certificate on the Appliance" on page 84 to generate the certificate. If you are using a certificate signed by a well-known Certificate Authority, you can skip this section.

To install a self-signed certificate on the mobile device:

1. Take the `name.cer` file that you generated in "Replacing the Default Certificate on the Appliance" on page 84 and email it to the user who has an email account configured on the mobile device. Alternatively, you could put it on a web or FTP site that is accessible from the mobile device.
2. Open the email (or web/FTP site) on the mobile device and tap the certificate attachment.
3. In the Install Profile window, tap **Install**.
4. Read the warning, then tap **Install**.
5. Verify that the certificate reads "Trusted" with a green check mark in the Profile Installed window.
6. (Conditional) If the certificate is not trusted, something is wrong with the certificate and the MobileAccess app will not work. Go back and try to generate the certificate again.
7. Tap **Done**.
8. Verify that this procedure worked by entering the appliance DNS name in the Safari address bar and ensuring that there is no warning about an untrusted certificate.

   NOTE: This step does not currently work in Chrome.

This certificate is installed on the Settings > General > Profiles page on the mobile device and can be removed from that location on the device.

The server certificate and the trusted root certificate need to be at least 2K in size.

After you have replaced the default certificate on the appliance, you can continue with MobileAccess installation and configuration.

Helping Users Register Their Mobile Devices

Users can install the MobileAccess app on a mobile device to use MobileAccess with CloudAccess. A user can register a device with multiple providers by setting up separate accounts for each one. If a user registers a device with multiple providers, the user must select the account to use for a session from the list of providers on the device. By default, the app connects the user to the first provider in the list.

Users must register their mobile devices to use MobileAccess with CloudAccess. As an administrator you can provide two different ways for users to register a mobile device with CloudAccess.

Registering iOS Devices

You can provide users with one of the following methods to register an iOS mobile device:

- **Manual URL Entry:** Send your users an email with the URL containing the DNS name of the appliance, including the correct port number. To enter the URL in the MobileAccess app, users tap the menu in the upper left corner of the app, then tap **Accounts** > **+** and enter the URL of the appliance in the **Providers** field. The URL is:

  ```
  https://appliance_dns_name:port
  ```

  For example:

  ```
  https://ias.example.com:8443
  ```

- **Embedded Link in Email:** Send your users the following link. When users click the link, the link launches the MobileAccess app and the Sign In page appears. Users sign in using their corporate credentials to access the appmarks available in the MobileAccess app. The link is:

  ```
  comnetiqauth://x-callback-url/register?providerUrl=https://
  appliance_dns_name:port/
  ```

  For example:

  ```
  comnetiqauth://x-callback-url/register?providerUrl=https://
  ias.example.com:8443/
  ```

  NOTE: Email clients can prevent embedded links from working.

Registering Android Devices

You can provide users with one of the following methods to register an Android device:

- **Manual URL Entry:** Send your users an email with the URL containing the DNS name of the appliance, including the correct port number. To enter the URL in the MobileAccess app, users tap the menu in the upper right corner of the app, then tap **Manage Accounts** > **+** and enter the URL of the appliance in the **Provider** field. The URL is:

  ```
  https://appliance_dns_name:port
  ```

  For example:

  ```
  https://ias.example.com:8443
  ```

- **HTML Page with Anchor Link:** Create an HTML page that contains an anchor link that users click to have the **Provider** field populated for them. The format of the anchor link is:

```
<html>
  <body><a href="intent://x-callback-url/register?providerUrl= https://
appliance_dns_name:port#Intent;scheme=comnetiqauth;package=com.netiq.mobileacc
essforandroid;end;">Register</a></body>
</html>
```

For example:

```
<html>
  <body><a href="intent://x-callback-url/register?providerUrl= https://
ias.example.com:8443#Intent;scheme=comnetiqauth;package=com.netiq.mobileaccess
forandroid;end;">Register</a></body>
</html>
```

Understanding the MobileAccess PIN

Administrators can require users to set a PIN on their mobile devices as a security measure to prevent unauthorized users from accessing protected resources through the MobileAccess app. Administrators can also specify whether users must re-enter the PIN after a period of inactivity on the device.

Users must install the MobileAccess app on the mobile device before they can set the PIN. If a PIN is required, the MobileAccess app prompts users to set the PIN the first time they open the app. Otherwise, users can set, change, or remove the PIN any time by accessing the Settings page from the MobileAccess app.

NOTE: The MobileAccess PIN is unrelated to the built-in device passcode, which is designed to protect other resources on the mobile device.

Even if the administrator does not require users to set a PIN, users can optionally set a PIN on their device. The PIN can be different for each mobile device the user registers. The PIN is not stored anywhere other than on the device itself.

Administrators can change the **Ask for pin** setting any time in the administration console. If the administrator specifies that a PIN is required after a mobile device has already been registered, the next time the user launches the MobileAccess app on the mobile device, the app prompts the user to set a PIN. The app then prompts the user for that PIN each subsequent time the user accesses the app. If the administrator initially requires users to set a PIN and then changes that requirement, users can remove the PIN from their device. However, the app does not notify users if a PIN is no longer required.

Whether the administrator requires users to set a PIN or a user chooses to set a PIN, by default users can enter their PIN incorrectly five times. On the fifth attempt, the application unregisters the mobile device and removes the current PIN. The user must then reregister the device and reset the PIN.

Unregistering Mobile Devices

Administrators who have the Device Administrator role in CloudAccess can manage and unregister user devices in the appliance administration console. So, if a registered mobile device is lost or stolen, or an employee leaves the company, you can ensure that unauthorized users cannot access corporate resources.

Users can also unregister their own mobile devices, either from their device or from the administration console. A mobile device that has previously been unregistered can be reregistered by the same user. However, for a different user to use the unregistered mobile device, the user must delete and reinstall the MobileAccess app on the device before reregistering the device.

The Devices page lists the devices for the logged-in user by default. If you are logged in with an account that has the Device Administrator role assigned, you have the option to search for and unregister devices that are registered to other users. If you log in with a regular user account, you can view and manage only your own registered devices.

To unregister mobile devices from the administration console as a Device Administrator user:

1. Log in to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click **Devices** at the top of the page.
3. (Conditional) If you want to search for the devices belonging to a particular user, enter the user name in the **User** field.
4. Click the trash can icon next to the device you want to unregister, then click **OK** on the confirmation message.

To unregister mobile devices from the Devices page as a regular user:

1. Browse to `https://`*`appliance_dns_name`*`/appliance/Devices.html`.
2. Enter your login credentials when prompted.
3. Click the trash can icon next to the device you want to unregister, then click **OK** on the confirmation message.

After a mobile device has been unregistered, the device can be registered to a new user. However, the MobileAccess app on the device must first be deleted and reinstalled.

11 Configuring Connectors

CloudAccess provides multiple connectors to SaaS applications. The connector for Google Apps for Business, the connector for Salesforce, the connector for ServiceNow, and the connector for Microsoft Office 365 enable both account provisioning and single sign-on (SSO). The other available connectors, which are downloadable from the Application Connector Catalog (catalog.netiq.com), provide only single sign-on capability.

The connectors for Google Apps, Salesforce, and ServiceNow are embedded in the appliance and are visible on the Admin page of the administration console as soon as you have initialized the appliance. The connector for Office 365 is included with the CloudAccess appliance. However, the administration console displays the connector only after you have installed the connector on the Windows server.

CloudAccess also ships with the connector for Bookmarks and the connector for OAuth2 Resources.

For more information, see the *CloudAccess Connectors Guide*.

12 Mapping Authorizations

Most companies define their business policies through authorization assignments. Examples of authorizations are groups, roles, and profiles. These authorizations are different depending on each SaaS application. For more information, see "Supported Roles and Authorizations" on page 91.

Authorizations give users access to resources. CloudAccess provides a simple solution that allows you to map your identity source roles (groups) to the SaaS application authorizations and approve or deny access to those authorizations.

Authorization categories are available for the connector types that provision users (Office 365, Google Apps, Salesforce, and ServiceNow). If you use connector types that provide only authentication and they require mapped authorizations for entitlements instead of Public access, their authorizations are available in the Other Applications category.

Policy mapping is an essential step in enabling user access to most applications. By default, the **Public** access option is disabled for all connectors except the connectors for Basic SSO. When you configure appmarks for a connector, if you leave the Public option disabled, no users can see the appmark on the landing page until you have mapped the application authorizations to desired identity source roles (groups) in Policy Mapping.

NOTE: Although CloudAccess allows you to map roles in social identity sources (such as Facebook) to provisioning SaaS applications (such as Google Apps), those mappings will not work. CloudAccess cannot provision users from any social media accounts, or from SAML 2.0 Inbound authentications. These are not full users in CloudAccess and cannot be provisioned.

The Policy Mapping page maps the authorizations from the SaaS applications to the roles (groups) in the identity sources and allows you to select whether the authorization requires an approval. If approval is required, the Approval page allows you to accept or deny the authorization request.

Supported Roles and Authorizations

Each identity source can contain different roles that appear on the Policy Mapping page:

- **Active Directory:** groups, local groups, and global groups
- **eDirectory:** group
- **Other Identity Sources:** roles for JDBC and SSUS identity sources

Each application contains different authorizations that appear on the Policy Mapping page:

- **Google Apps:** user and groups
- **Office 365:** account, groups, and license
- **Salesforce:** groups, roles, and profiles (account types)
- **Other Applications:** appmarks for Bookmarks or other applications that require mapped authorizations for entitlements instead of Public access.

Provisioning applications support mapped authorizations only for users in Active Directory, eDirectory, and JDBC identity sources. For more information, see "Requirements for Provisioning" in the *CloudAccess Connectors Guide*.

Prerequisites

Verify that you meet the following prerequisites before mapping SaaS application authorizations to the identity source groups:

- ❒ Configure the appropriate connectors for your environment. For more information, see Chapter 11, “Configuring Connectors,” on page 89.
- ❒ Ensure that roles (groups) in the identity source exist.
- ❒ Populate the required attributes on the users in the identity source. For more information, see Chapter 4, “Configuring LDAP and JDBC Identity Sources,” on page 37.

Loading Authorizations

To map an authorization, you must load the authorization into the Policy Mapping page.

To verify that applications are available for mapping authorizations:

1. Verify that you have configured the SaaS application connectors that provision users.

   For more information, see Chapter 11, “Configuring Connectors,” on page 89.
2. Log in to the administration console using the application administrator credentials you specified when you created the SaaS application connector.
3. Click **Policy** to open the Policy Mapping page.
4. In the right pane, click the down arrow next to the connector, then select your SaaS application connector, or select **Other Applications** and select the application.

   If the Policy Mapping page does not display the SaaS application connector, you did not configure the connector properly. For example, if the **Public** policy is enabled for a connector, the application does not appear in the list. For more information, see Chapter 11, “Configuring Connectors,” on page 89.

Successfully completing these steps populates the Policy Mapping page with the SaaS application’s authorizations.

Reloading Authorizations

When you perform a switch master with the cluster nodes, or if authorizations change in the SaaS applications, or you add new roles in the identity sources, you must reload the authorizations on the Policy Mapping page.

To reload authorizations:

1. To reload roles (groups) from the identity sources, click the **Reload table** icon ⟳ at the end of the Identity Source table.
2. To reload authorizations from the SaaS applications, click the **Reload table** icon ⟳ at the end of the Authorizations table.

Mapping Authorizations

After the authorizations load, map the SaaS application authorizations to the identity source roles (groups). You can use filters in the search fields at the bottom of the window to filter applications and identity source roles.

NOTE: If you use wildcards such as an asterisk (*) or question mark (?) in the search filter field, CloudAccess does not correctly filter results. Filters must be full regular expressions. If you want to use wildcards, they must be regular expression wildcards. If the filter does not start with '^' and `'.*'`, then `'.*'` is added to the filter. If the filter does not end with '$' and `'.*'`, then `'.*'` is added to the filter. Thus, a filter for "`test`" would end up as the regular expression "`.*test.*`".

To map authorizations:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click **Policy** at the top of the page.
3. In the right pane of the Policy Mapping page, click the down arrow, then select the desired SaaS connector, or select **Other Applications** and select the application.
4. In the **Role Name** column on the left, select the role (group) from the identity source you want to map to an authorization from the selected SaaS connector.
5. In the right pane, drag and drop the desired authorization from the SaaS connector to the left mapping pane.

   or

   In the left pane, drag and drop the desired group from the identity source to the right mapping pane.
6. (Optional) Click the **Approvals** icon to specify that an approval is required to grant access.

   We recommend a maximum of 2,000 simultaneous approvals. For more information about approvals, see "Approving Requests" on page 95.
7. Click **OK** to map the SaaS authorization to the identity source group.

The mapping grants access for users who are members of the identity source roles to the SaaS application authorization. When you add new users to the role (group) that is mapped to a SaaS account authorization, and the request is then approved (if approval is required), the users will see the associated appmark on the landing page or the MobileAccess application page. If the **Prompt users for an existing account before provisioning** option is enabled (available only for Salesforce), users are prompted to create a new SaaS account or to claim an existing account the first time they click or tap the appmark. If that option is not enabled, the accounts are provisioned automatically. For information, see "How CloudAccess Provisions User Accounts" in the *CloudAccess Connectors Guide*.

NOTE: If you map a group to a role in CloudAccess and the group is subsequently removed from scope or deleted from the identity source, CloudAccess removes the policy mappings as well. If you recreate the group or add it back to the scope, you must remap the group to the appropriate role on the Policy Mapping page in CloudAccess.

Understanding Google Apps Mappings

Mapped placement of newly provisioned users to a sub-organization overrides the default placement in the top-level organization. On the Policy page, you can map the User Account authorization and a User Placement authorization value to the same identity source group. After users are added to the appropriate identity source group, which triggers user account provisioning to Google Apps, new users are placed in the organization that you mapped to the identity source group in Policy Mapping.

IMPORTANT: Pay careful attention when mapping User Placement authorization values to identity source groups on the Policy page to ensure that users are placed in the intended Google Apps organizations. Google Apps allows each user to be placed in only one organization at a time. If you grant a User Placement authorization to a user, and then grant another User Placement authorization to the same user, the first value is overwritten when the user is moved in the Google Apps organizational unit structure.

In addition, if you revoke a User Placement authorization for a user, even if that user has multiple User Placement authorizations, that user is moved to the default organization specified in the Google Apps connector configuration. (Because Google Apps allows a user to be placed into only one organization at a time, when a User Placement authorization value is overwritten, there is only one value that is removed, which moves the user back to the default placement.) If you want to move that user from the default location back into a new Google Apps sub-organization, you must add the user back to the appropriate identity source group and perform policy mappings again.

If you revoke a User Account authorization for a user after the user has been provisioned into Google Apps and one or more User Placement authorizations have been granted to the user, that user is placed in suspended mode in Google Apps. No placement activity takes place as long as the user account is suspended; the user simply remains in the Google Apps organization that they were in before the suspension. When you re-grant the User Account authorization, the account is moved to the "active user" state. If you performed a User Placement authorization change while the user account was suspended, the user is moved to the appropriate organization after the account is reactivated.

A Mapping Example

Use the following example of authorization mapping in Google Apps to understand how mapping works.

1 In Active Directory:

  1a Create a group named GoogleAppsUsers.

  1b Add users to the GoogleAppsUsers group.

2 In Google Apps for Business, create a Google Apps Account group.

3 In CloudAccess, configure the connector for Google Apps.

4 On the Policy Mapping page:

  4a Load the authorizations for the connector for Google Apps.

  4b In the **Role Name** column, select the connector for Active Directory.

  4c In the right pane, select the connector for Google Apps.

  4d Drag and drop the Google Apps Account into the left pane, over the GoogleAppsUsers group.

4e Click **OK**.

The appliance automatically provisions all users in the GoogleAppsUsers group to the Google Apps Account group.

5 In Active Directory, create a new user, then add the user to the GoogleAppsUsers group.

The user is automatically added to the Google Apps Account group and has access to Google Apps for Business.

Approving Requests

CloudAccess provides the ability to approve or deny requests to the SaaS applications. During the configuration of the connector, you specified an application owner. The application owner approves or denies requests for access to the SaaS applications. The application owner knows who should have access to the SaaS applications, whereas the appliance administrator might not have this knowledge.

The **Approval** icon appears in the administration console only if you have mapped roles and selected the option to require approval for the account. When there are accounts waiting for approval, CloudAccess adds the **Approval** icon.

By default, CloudAccess automatically provisions users according to mapped authorizations. To enable approvals so that automatic provisioning does not occur, click the **i** (Configure Authorizations Policies) icon when you map the roles (groups) from the identity source to the SaaS applications authorizations on the Policy Mapping page. Now an application owner must grant approval before provisioning can occur.

You can use filters in the search field at the bottom of the Approval window to filter approval requests.

NOTE: If you use wildcards such as an asterisk (*) or question mark (?) in the search filter field, CloudAccess does not correctly filter results. Filters must be full regular expressions. If you want to use wildcards, they must be regular expression wildcards. If the filter does not start with '^' and '`.*`', then '`.*`' is added to the filter. If the filter does not end with '$' and '`.*`', then '`.*`' is added to the filter. Thus, a filter for "`test`" would end up as the regular expression "`.*test.*`".

To grant or deny approval:

1. Log in to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html` as the application owner.
2. Click the **Approval** tab.
3. Select one or more approval requests.

   We recommend that you select fewer than 300 requests in a single accept or deny action. Otherwise, when approving or denying a large number of workflow requests in a single action, the amount of memory used by the browser can cause the page to become unresponsive and the browser to close.
4. Click **Approve** or **Deny**.

NOTE: Users who have been deleted from the identity source might still appear on the Approval page. If you know that certain users have been deleted, you can simply deny approval for those users. However, approving requests for users who have been deleted does *not* result in account provisioning for those users in the SaaS applications.

13 Reporting

CloudAccess provides reports of users' activity through the appliance. You can run, download, and save various reports on the **Reports** tab in the administration console.

CloudAccess provides the option to use Google Analytics as an external dashboard, and you can also configure CloudAccess to forward events to Sentinel Log Manager or a syslog server to help troubleshoot various issues. Event types that are forwarded include Login, Logout, Register Device, Un-register Device, and Failed Login.

Using Google Analytics as an External Dashboard

CloudAccess enables administrators to use Google Analytics as an external dashboard to monitor and analyze CloudAccess usage. After you have completed the free Google Analytics registration process for the CloudAccess appliance, data is available for analysis within a few hours. You can also do your own data mining with the API that Google provides. For more information, see the Google Analytics website (http://www.google.com/analytics/?gclid=CJCt792Y07kCFUlp7AodDBwALA).

To set up Google Analytics for CloudAccess:

1. (Conditional) If you do not already have a Google account, set one up on the Google website.
2. Sign in to your Google account and select the option to register for Google Analytics.
3. Select the option to monitor a website and provide the base URL for the CloudAccess appliance. Google Analytics tracks both user and admin logins. For example, `https://`*`appliance_dns_name`*.
4. Specify an account name. This account name is only for managing Google Analytics and does not affect anything in CloudAccess. You can share this account name as needed.
5. Log in to the CloudAccess administration console.
6. On the Admin page, drag the Google Analytics icon from the **Tools** palette to the **Tools** panel.
7. Enter the Tracking ID (not the tracking code) that Google provided during the registration process and click **OK**.
8. Click **Apply** and wait for the appliance to update.

NOTE: If you have any issues with configuring the Google Analytics tool in the administration console, such as the tool being invisible on the Tools palette, verify that you do not have any ad blockers running in your browser that might be interfering with administration tasks. You should be able to disable any ad blockers on the web page itself.

Integrating with Sentinel Log Manager

The CloudAccess appliance can forward events to Sentinel Log Manager 1.2.x if you want more detailed reports.

To integrate the appliance with Sentinel Log Manager:

1. Configure Sentinel Link in Sentinel Log Manager.

For more information, see Sentinel Link Overview Guide (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html).

2 Open TCP port 1290 on the Sentinel Log Manager server.

   2a To change the port, use `ssh` and log in to the Sentinel Log Manager server as `root`.

   2b At the command prompt, enter `yast firewall`.

   2c Select **Advanced** > **Allowed Services**, then manually add port 1290 to the list of TCP ports.

3 On the Admin page in CloudAccess, drag the **Sentinel** icon from the **Tools** palette to the **Tools** panel.

4 Click the Sentinel icon, then click **Configure**.

5 Specify the IP address and port of the Sentinel Link server, then click **OK** and **Apply** to save the changes.

The CloudAccess appliance appears as another event source in Sentinel Log Manager.

Configuring CloudAccess to Forward Events to a Syslog Server

You can configure CloudAccess to forward various events to a syslog server to help troubleshoot various issues. Event types that are forwarded include Login, Logout, Register Device, Un-register Device, and Failed Login.

To configure CloudAccess to forward events to a syslog server:

1 Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

2 Drag the **Syslog** tool from the **Tools** palette to the **Tools** panel.

3 In the **Tools** panel, click the Syslog tool, then click **Configure**.

4 Specify the IP address and the port of the syslog server.

5 Select the type of protocol to use: **UDP**, **TCP**, or **TLS**.

6 Click **OK** to save the tool settings.

7 On the Admin page, click **Apply** to activate event forwarding.

14 Configuring the End User Experience

CloudAccess allows you to configure the end user’s email client or mobile devices to use the single sign-on authentication to access the SaaS applications. This increases the security of your company’s information stored in the SaaS applications because users authenticate with their corporate credentials, but these credentials are never stored in the SaaS applications.

Configure each user’s email client or mobile device to point to the CloudAccess appliance. The appliance acts as a proxy, so when users access the SaaS applications, the appliance automatically logs users in to the SaaS application.

CloudAccess also allows you to customize the login, logout, and landing pages so they display your company’s branding instead of the default branding.

Configuring Email Clients

You can configure any supported email client to point to CloudAccess. The email clients allow you to receive email from multiple sources in one location. For a list of supported clients, see “Email Clients” on page 20.

NOTE: The following procedure lists typical ports for email clients, but ports might vary depending on your environment.

To configure your email client to use a CloudAccess email account:

1. Access your email client.
2. Create a new email account using the following information to configure CloudAccess as your email source:

   Incoming email server (IMAP/POP): Specify the IP address or hostname of your appliance.

   Incoming email server username: Specify your identity source enterprise logon name for the account name.

   Incoming email server password: Specify your identity source password.

   If your password changes, you must change the password in the email account.

   Outgoing email server (SMTP): Specify the IP address or hostname of your appliance.

   SSL: You must select **SSL** for IMAP (port 993), POP (port 995), and SMTP (port 25).

   The SMTP server requires authentication.

   For more information, see the appropriate documentation for the email client you are using.

Enabling Google Mail Proxy

For users to have access to Google Apps Mail from supported mobile devices, you must first enable the option in CloudAccess and then instruct your users to perform some additional configuration steps in Google Apps. For more information about enabling the option in CloudAccess, see “Enabling Google Mail Proxy” in the *CloudAccess Connectors Guide*.

NOTE: There is currently no way for Google administrators to set the IMAP and security settings for the whole domain. The settings are on an individual account basis, so end users must perform the steps in the following procedure for their own Google Apps accounts to enable mail proxy for mobile devices.

To enable mail proxy for mobile devices:

1. Log in to your Google Apps account through CloudAccess to enable the account, and accept the terms and conditions.
2. Click the **Settings** (gear) icon in the top right corner.
3. Click the **Forwarding and POP/IMAP** tab, then select **Enable IMAP**.
4. Click **Save Changes**.
5. Click the **Accounts** tab, then click **Google account settings**. The Sign-in & security options open in a new browser window.
6. In the navigation pane under **Sign-in & security**, click **Connected apps & sites**.
7. Switch the **Allow less secure apps** option to `ON`.

Configuring End User Browsers for Kerberos Authentication

If you are using Windows Integrated Authentication for Kerberos authentication to CloudAccess, each end user browser must be configured to use Kerberos authentication.

For information about configuring Kerberos, see "Configuring Integrated Windows Authentication with Kerberos" on page 69.

To configure Kerberos authentication for web browsers:

1. Add the user computers to the Active Directory domain.

   For instructions, see your Active Directory documentation.
2. Log in to the Active Directory domain, rather than the computer.
3. (Conditional) If you are using Internet Explorer, configure the browser to trust the appliance:

   3a Click **Tools** > **Internet Options** > **Security** > **Local intranet** > **Sites** > **Advanced**.

   3b In the **Add this website to the zone** field, enter the Base URL for the appliance, then click **Add**.

   In the configuration example, this URL is `serv1.example.com`.

   3c Click **Close**, then click **OK**.

   3d Click **Tools** > **Internet Options** > **Advanced**.

   3e Verify in the Security section that **Enable Integrated Windows Authentication** is selected, then click **OK**.

   3f Restart the browser.
4. (Conditional) If you are using Firefox, configure the browser to trust the appliance:

   4a In the URL field, specify `about:config`.

   4b In the **Filter** field, specify **network.n**.

   4c Double-click `network.negotiate-auth.trusted-uris`.

This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser. Specify a comma-delimited list of trusted domains or URLs.

For this example configuration, add `serv1.example.com` to the list.

4d Click **OK**, then restart your browser.

Customizing Branding on User-Facing Pages

CloudAccess allows you to customize user-facing pages, such as the login page, so users see your company branding instead of the default branding. After you have customized those pages, you can modify them as needed to meet new company requirements. Customizing the user pages does not affect any pages in the administration console itself.

If you implement custom branding in your CloudAccess environment and then re-run the initialization process to modify the DNS server or make other changes to an existing cluster, branding is reset to the default settings. Before you re-run the initialization process on an existing cluster, ensure that you back up your customized branding files so that you can reuse them.

IMPORTANT: Performing advanced branding customization requires advanced JavaServer Pages (JSP) knowledge. Before you make any changes, ensure that you have a good snapshot of your appliance that you can revert to if necessary. If you upload a bad branding file and are unable to log in to the administration console, you can re-run the appliance initialization to restore the default login pages. For more information, see "Initializing the Appliance" on page 23.

To customize branding for users:

1 (Conditional) If you plan to perform extensive rebranding, take a snapshot of the appliance.

2 Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

3 On the toolbar, click the Tools icon, then click **End user branding**.

4 (Conditional) If you want to customize the user login page, complete the following steps:

4a Click **Basic Customization**.

4b Change the title and background colors by specifying HTML color codes.

4c Change the default image by either not showing the image, or uploading a new image.

The image size on the user landing and logout pages is always scaled to 60 x 60. On the login page, if the specified image is between a minimum of 60 x 60 and a maximum of 300 x 300, CloudAccess displays the image "as is." If the image is outside this range, CloudAccess scales it to the nearest minimum or maximum value.

4d Click **OK** to save the changes and then click **Apply**.

5 (Conditional) If you want to perform more extensive rebranding, complete the following steps:

5a Click **Advanced Customization**.

5b Click **Download default end user login code**.

5c Save the file to your local computer.

5d Save a backup copy of the file.

5e Unzip the downloaded file and locate the `.jsp` files in the `osp\jsp` subdirectory.

5f Modify the desired JSP pages. The default text for the login page is located in the `osp\resources\oidp_custom_resources_en_US.properties` file.

For more information about the JSP files, see Appendix A, “Performing Advanced Branding,” on page 121.

5g Zip up the files again. Include only the `images` and `jsp` directories, but ensure that you keep them in the original `osp` directory.

5h Log in to the CloudAccess console again.

5i On the toolbar, click the Tools icon, then click **End user branding**.

5j (Conditional) If you are customizing pages for the first time, click **Browse**, then browse to and select the modified file.

5k (Conditional) If you are updating previously customized pages, delete the name of the existing file. Click **Browse**, then browse to and select the `.zip` file that contains the newly modified`.jsp` files.

5l Wait until the **Delete** button appears, then click **OK**.

If rebranding was unsuccessful, an error message will appear.

5m Click **Apply**.

The pages now display the branding you customized in the `.jsp` files.

Configuring User Session Timeouts

The user session timeout is set to 10 minutes by default, but it is configurable.

NOTE: The admin session timeout is set to 10 minutes and is not configurable.

To change the user session timeout:

1. On the Admin page, click the cluster icon at the bottom of the page, then click **Configure**.
2. Adjust the setting in the **User session timeout** field as needed, then click **OK**.

15 Maintenance Tasks

CloudAccess allows you to change various appliance configuration settings as needed. For example, moving your appliance from a staging configuration to a production environment requires changes to the networking components.

Changing the Cluster Password

You set the appliance administrator password in the last step of the initialization process, but you can change the password as needed. The administrator password is the same for all nodes in the cluster.

To change the cluster password:

1. On the Admin page, click the cluster icon at the bottom of the page, then click **Change cluster password**.
2. Type your old password, then type your new password twice and click **OK**.

NOTE: You can also change the appliance administrator password if you re-initialize the appliance. For more information, see "Changing Initialization Settings" on page 24.

Changing the IP Address

You can change whether a node uses a DHCP IP address or a static IP address on the Admin page.

To change the IP address:

1. Click the node icon, then click **Configure**.
2. Select whether the appliance uses a DHCP IP address or a static IP address.

   If you select to use a static IP address, you can change the required values for the subnet mask, default gateway, and the DNS server.
3. Click **OK** to save the changes.
4. Click **Apply** to apply the changes to the appliance.

Changing the Public DNS Name or NTP Server Settings, or Uploading New Certificates

The appliance contains self-generated certificates. You can upload custom certificates through this interface. You can also change the public DNS name or NTP server if necessary.

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click the cluster icon under **Appliances**, then click **Configure**.
3. Change the key pairs, NTP server, or public DNS name, then click **OK**.
4. Click **Apply** to apply the changes to the appliance.

Expired key pair certificates prohibit changes from being made to this page and make the key pair field red. If the key pair expires, you must re-initialize the appliance before you can upload a new certificate.

Updating the Appliance

CloudAccess provides an update channel for keeping your appliances current with the latest security fixes, bug fixes, and patch updates. Updates work only if you have registered each node in the cluster. For more information, see “Registering the Appliance” on page 26.

When an update is available for one or more nodes in the cluster, the CloudAccess Admin page displays a flag icon in the upper right corner of the window. You can also configure the appliance to send an email notification when an update is available. When you click the flag icon, you can see the version of the pending update, instructions on how to apply the update, and the Release Notes associated with the update.

The flag icon for the update channel appears only if you are logged in to the Admin page with an administrator account. Other consoles do not display the flag icon.

CloudAccess automatically checks the update channel for updates once daily at 11:23:23 p.m. and downloads any available update. You can also manually check for updates any time by clicking **Tools > Check for updates** on the Admin page. You can download and install an update as soon as the flag appears on the Admin page, or you can wait for CloudAccess to download the update that night, to minimize network impact due to possible size of an update.

WARNING: We recommend that you download and install an update in two separate steps. If you download and update in the same step and the download is interrupted or incomplete, the update fails. The appliance might become unresponsive or seem to be in a restart loop. If this occurs, download the update, then go back to the snapshot and try again to apply the update.

Always keeping your appliance up to date is a best practice. However, updates are cumulative, so if you miss an update you can just install the next one when it is available.

IMPORTANT: If you apply an update to one node, you must apply the update to all the other nodes in the cluster. Update one node at a time. Ensure that the update was successful and the node is still working properly before you begin updating the next node. Do not perform any other administrative tasks that require an **Apply** command, and do not switch the master node, until all nodes have been successfully updated to the same version of CloudAccess.

This process allows you to run in a mixed environment while you update each node. After you have applied all available channel updates, the flag icon goes away.

To apply an update:

1. Take a snapshot of each node in the cluster to create a backup.
2. Click the desired node, then click **Apply update**.

   CloudAccess displays status messages during the installation of the update and the rebooting of the node.
3. After the update completes and the node restarts, click **About** on the node to verify the updated version.
4. Verify the health of the updated node and all of the nodes in the cluster. Ensure that all icons are green.

For more information, see "Displaying Health" on page 107.

5 Repeat Step 2 through Step 4 for each node in the cluster.

6 When you are sure that all of the nodes in the cluster are working as expected, delete the snapshot.

Shutting Down or Rebooting a Node

You can shut down or reboot a node in the cluster if necessary.

NOTE: If you shut down the node in a single node cluster, the administration console becomes inaccessible. You must then use the hypervisor management tools to power on the node. Similarly, if you reboot the node in a single node cluster, the administration console is inaccessible until the reboot is complete.

To shut down or reboot a node:

1 Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.

2 Click the node that you want to shut down or reboot, then click **Shutdown/Reboot** on the menu.

3 In the confirmation window, click **Shutdown** or **Reboot**.

4 (Conditional) Wait for the node to reboot, or use the hypervisor management tools to power the node back on.

Recovering from a Disaster

Use snapshots of the nodes to recover from a disaster. It is important to take snapshots of each node in the cluster regularly so you do not lose information.

To prepare for and recover from a disaster:

1 Take a snapshot of each node in the cluster, within a short time. It is not necessary to shut down the working nodes when taking snapshots.

IMPORTANT: Do *not* select the **Snapshot the virtual machine's memory** check box when you take the snapshot. Including the memory in the snapshot can cause issues when restoring from snapshot.

2 When a failure happens, restore the master node snapshot first.

3 Restore the other nodes in the cluster.

Use these steps only for disaster recovery. Never restore one snapshot. CloudAccess contains a database that is time-sensitive. Restoring only one node and not the others causes corruption in the appliance.

16 Troubleshooting CloudAccess

The CloudAccess administration console displays health status information for the system, the nodes, and the cluster on the Admin page. This section describes the health status indicators, how to troubleshoot health issues, and how to work around known issues.

Troubleshooting the Appliance Initialization

If the appliance initialization fails, the user interface displays a link for log files. Click the link to download the log files that provide information about the failure.

Displaying Health

CloudAccess displays health status information for each node and for the cluster at the bottom of the Admin page. Hover the mouse over each node to display the health status of the node. If you want more details, click the node, then select **Show Health.** CloudAccess refreshes health status information every five minutes.

When you click **Show Health**, CloudAccess displays the status for each component of the appliance. If the status is anything other than green (healthy), use the troubleshooting tools to determine what is wrong.

Using Troubleshooting Tools

CloudAccess provides troubleshooting tools to help you resolve problems.

To access these tools:

1. Log in with an appliance administrator account to the administration console at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Under **Appliances**, click the node icon, then click **Enter troubleshooting mode**.
3. Click the node icon again, then click **Troubleshooting tools**.
4. Select one or more of the troubleshooting scenarios listed.
5. Duplicate the error or condition.
6. Click **Download CloudAccess Log Files** to download the logs.

IMPORTANT: After you obtain the logs, turn off troubleshooting mode by clicking the node icon again and then clicking **Exit troubleshooting mode**. Leaving the logs running affects the performance of your appliance.

All of the log files in Table 16-1 are included in the download, no matter what scenario you select. The scenario you select determines the amount of data displayed in the log files. Search the appropriate log file for errors while troubleshooting issues.

Table 16-1 Troubleshooting Log Files

Feature	Logs

Initialization or commands	`ConfigurationReplicator.log`
	`ConfigurationReplicator_RL.log`
	`messages`
	`boot*`
	`packageoperations.log`
	`dserv.log`
	`firewall`

Forward proxy	`access.log`
Admin.html UI	`adminui.log`
Registration	`register.log`

Updates	`zypper.log`
	`downloadUpdate.log`
	`afterUpdate.log`
	`beforeUpdate.log`
	`rpmsAfterUpdate.log`
	`rpmsBeforeUpdate.log`
	`rpmsUpdateDiff.log`
	`300_appliance_SnapshotUconPackages.sh.log`

Identity Source Provisioning	`bis_AD_<`*xxxxx*`>.log`
	`bis_AD_<`*xxxxx*`>_RL.log`
	`ConnectorLogs.txt`
	`bis_EDIR_h2q3p.log`
	`bis_EDIR_h2q3p_RL.log`

Provisioning to the SaaS Applications	`connectors_SFORCE_<`*xxxxx*`>_RL.log`
	`connectors_GOOGLEAPPS_<`*xxxxx*`>.log`
	`connectors_GOOGLEAPPS_<`*xxxxx*`>_RL.log`
	`connectors_O365_<`*xxxxx*`>.log`
	`connectors_O365_<`*xxxxx*`>_RL.log`
	`connectors_SERVICENOW_<`*xxxxx*`>.log`
	`connectors_SERVICENOW_<`*xxxxx*`>_RL.log`
	`ConnectorLogs.txt`

Feature	Logs
Mapping	`RolesandResourceServiceDriver.log`
	`UserApplicationDriver.log`
Approvals	`jboss.log`
Reporting	`ManagedSystemGatewayDriver.log`
	`DataCollectionServiceDriver.log`
Mobile Devices	`mail`
	`mail.err`
	`mail.info`
Custom Connectors	`catalina.out`
End User Authentication	`catalina.out`

Troubleshooting Different States

CloudAccess displays indicators for the current state of the different appliance components. The display refreshes every five minutes. CloudAccess might not immediately display the change.

The following sections list the different components, the possible states, and troubleshooting steps you can take when the state changes.

- "Master Node Health" on page 109
- "Front Panel of the Node" on page 109
- "Top of the Node" on page 110
- "Identity Source" on page 111
- "Applications" on page 112
- "Tools" on page 112

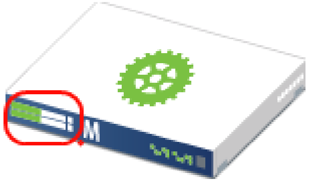
Master Node Health

The master node is responsible for all administration functions in CloudAccess. If the master node is not running, the following functions do not work: provisioning or deleting user accounts, mapping authorizations, system roles, approving requests, and reporting. Other nodes in the cluster continue to capture and cache events, but they do not send those events to the master node until it is running again. Similarly, event forwarding to Sentinel does not work as long as the master node is down.

Front Panel of the Node

The indicator on the front panel of the node displays the health state of the node.

Figure 16-1 Front Panel



The states are:

Green: The node is healthy.

Yellow: The node cannot communicate with the other nodes within the five minute refresh.

Red: The node cannot communicate with the other nodes within two of the five minute refresh cycles.

Clear: The node is initializing or the state of the node is unknown.

Perform the following troubleshooting steps in the order listed if the state is anything but green:

1. Wait at least five minutes for the display to refresh and display the current state.
2. Click the node, then select **Show health**.

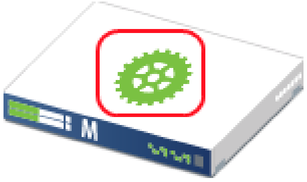
   Show Health displays which part of the appliance is having issues.
3. If Show Health displays a problem, use the troubleshooting tools to gather logs.

   For more information, see "Using Troubleshooting Tools" on page 107.
4. Restart the appliance, then wait at least another five minute cycle for all nodes to display the current state.

Top of the Node

The indicator on the top of the node shows whether the **Apply** commands completed successfully.

Figure 16-2 Top of the Node



The states are:

Green: All **Apply** commands completed successfully.

Red: The **Apply** commands did not complete successfully.

Perform the following troubleshooting steps in the order listed if the state is red:

1. Mouse over the top of the node to see the status of the last **Apply** command made on the node.
2. If there is not enough information in the summary, click **Enter troubleshooting mode** on the node, then mouse over the node again.

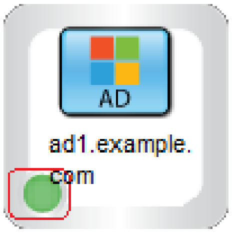
The troubleshooting mode displays a detailed summary of the last **Apply** command made on the node.

3. Restart the appliance, then wait at least another five minute cycle for all nodes to display the current state.

Identity Source

The health indicator for the identity source is the small icon in the lower left corner.

Figure 16-3 Identity Source Indicator



The states are:

Green: The connector to the identity source is healthy.

Yellow: The connector has communication problems with the identity source.

Red: The connector to the identity source is unhealthy or contains errors.

Question mark: The state of the connector to the identity source is unknown.

Perform the following troubleshooting steps in the order listed:

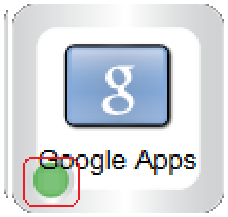
1. If the connector is green, but the CloudAccess interface is not displaying users, verify that the identity source servers are running and communicating properly.
2. Use the troubleshooting tools to gather logs, then look at the identity source provisioning logs listed in Table 16-1 on page 108 for errors. The `ConnectorLogs.txt` file maps the display name of the connector with the log name of the connector, if there is more than one identity source connector.
3. Click **Show health** on the master node, then expand **Operational**.

   If these items are yellow or red, the interface displays helpful information to help troubleshoot the issue.
4. If you are using LDAPS to communicate with the identity source, verify that the LDAP certificates are not expired. You refresh the certificates as follows:
   a. Log in to the CloudAccess administration console, then click **Configure** on the identity source.
   b. Click the **Refresh** icon next to the identity source server.

Applications

The health indicator for an application connector is the small icon in the lower left corner.

Figure 16-4 *Application Indicator*



The states are as follows:

Green: The connector to the application is healthy.

Yellow: The connector to the application contains warnings.

Red: The connector to the application contains errors or cannot communicate with the application.

Question mark: The connector to the application is in an unknown state.

Perform the following troubleshooting steps in the order listed:

1. Click **Show health** on the master node, then expand **Operational**, and check the status of **Provisioning**.

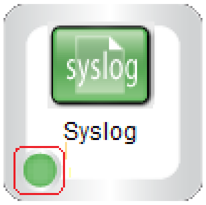
   If **Provisioning** is yellow or red, CloudAccess displays helpful information to help troubleshoot the issue.
2. Use the troubleshooting tools to gather logs, then look at the provisioning logs listed in Table 16-1 on page 108 for errors.
3. Make a cosmetic change to the application connector configuration, then click **Apply**.

   By forcing an **Apply**, the appliance refreshes the application connector state and this can resolve the issue.

Tools

The health indicator for a tool is the small icon in the lower left corner. Only tools that report health have an indicator. The following tools do not have a health indicator: Google Analytics, Mobile, and Time-Based One-Time Password (TOTP).

Figure 16-5 *Tool Indicator*



For all tools, the **Question Mark** icon indicates that the tool is in an unconfigured state.

Advanced Authentication: The states for the Advanced Authentication tool are as follows:

- **Green circle:** The connection to the Advanced Authentication appliance is healthy, and only Active Directory identity sources exist in the configuration.
- **Yellow triangle:** The connection to the Advanced Authentication appliance is healthy. The triangle indicator serves as a warning that identity source types other than Active Directory exist in the configuration and are not supported with the Advanced Authentication authentication providers.
- **Red circle:** The connection to the Advanced Authentication appliance is not working. The Advanced Authentication server is unreachable.

Forward Proxy: The states for the Forward Proxy tool are as follows:

- **Yellow triangle:** The connection to or through the proxy is healthy. The triangle indicator serves as a warning that use of Forward Proxy is intended for test environments only.
- **Red circle:** The connection to or through the proxy is not working. The proxy device is unreachable.

Google reCAPTCHA: The states for the Google reCAPTCHA tool are as follows:

- **Green circle:** All of the configured identity sources are valid for use with reCAPTCHA.
- **Yellow triangle:** One or more of the configured identity sources are not valid for use with reCAPTCHA. For more information, see "Requirements for reCAPTCHA" on page 71.
- **Red circle:** None of the configured identity sources are valid for use with reCAPTCHA.

Sentinel and Syslog: The states for the Sentinel and Syslog tools are as follows:

- **Green circle:** The connection to the specified address:port is healthy.
- **Red circle:** The connection to the specified address:port is not working.

Understanding Support for International Characters

CloudAccess supports the use of international characters in values for identity attributes, except where the related identity source or application does not allow them. The international character can cause the authentication-related CloudAccess transaction to fail. For example, CloudAccess might be unable to provision a user's application account or to create a new account in an SSUS identity source.

Table 16-2 identifies the identity attributes for external components that do not support using international characters.

Table 16-2 *Known Issues for International Characters in Identity Sources and Applications*

External Component	Does not support international characters for...
Identity Sources	
Active Directory	The email attribute value
Self Service User Store	The email address used as the user name for an account
Applications	
Any external OAUTH2 service	The user attribute

External Component	Does not support international characters for...
Google Apps for Business	The cn and sAMAccountName attribute values
Office 365	The cn and sAMAccountName attribute values
Salesforce	The email attribute value

Troubleshooting Provisioning Issues

Use the information in the following sections to troubleshoot provisioning issues.

Capturing Logs for Provisioning Issues

By default, when you provision users, the appliance does not log any information about the provisioning process. Enabling logging causes performance issues, so you should never leave the logging running all of the time.

However, if you have provisioned users and select accounts are not showing up in the SaaS applications, you will need to enable logging to capture the cause.

To capture logs of provisioning issues:

1 Determine which account (or accounts) were not provisioned.

2 Remove that account from the group that grants access to the SaaS application.

3 Turn on logging:

  3a Access the Admin page of the appliance console.

  3b Under **Appliances**, click the **Node** icon, then click **Enter troubleshooting mode**.

  3c Click the **Node** icon again, then click **Troubleshooting tools**.

  3d Select **Provisioning**, then click **Apply** and **OK**.

4 Add the user to the group or initiate the provisioning action.

5 Access the troubleshooting tools again.

6 Click **Download CloudAccess Log Files** to download the logs.

7 Deselect **Provisioning**, then turn off troubleshooting mode.

8 Review the logs to find the error when provisioning occurs.

Ensure that you have turned off troubleshooting mode, otherwise it will cause performance problems with the appliance.

Understanding the Result of Actions Performed on Users and Groups

Actions that are taken on users and groups in the identity source might not be reflected in the SaaS applications (Google Apps, Salesforce, ServiceNow, and Office 365). The following table lists the actions in the identity sources and the corresponding actions in the SaaS applications.

Table 16-3 Provisioning Actions

Identity Sources	SaaS Applications
Delete a user. (Or disable a user account.)	Disables the SaaS account. **NOTE:** In the MobileAccess app on an iOS device, the user continues to have access to the SaaS account until the in-progress user session times out.
Remove a user from the authorized group.	Disables the SaaS account.
Create a user.	- Creates an account for the user in the SaaS application, if the user is a member of a group with mapped SaaS authorizations. or - Users are prompted to validate their information when they log in the first time.
Move a user from out of the search context into the search context.	Creates an account for the user in the SaaS application, if the user is a member of a group with mapped SaaS authorizations.
Move a user out of the search context.	Disables the SaaS account.

By default, CloudAccess establishes identity based on an internal unique ID in the identity source, not based on the user name, and does not support recreating users with the same name unless they also have the same internal unique ID. Once a user has been mapped and provisioned, if you delete the user from the identity source and then recreate that user with the same name, you will not be able to cache and activate the user in CloudAccess or provision the user to SaaS applications. When CloudAccess is unable to cache users properly, the Cached User Status Bar indicates this status with a lower number of active users than cached users.

IMPORTANT: CloudAccess does provide a **Relaxed user matching** option under **Advanced Options** on the configuration window for the identity source. If you select this option, CloudAccess matches users based on CN or sAMAccountName instead of the internal unique ID. This option enables you to recreate previously deleted users so CloudAccess can manage them again, but you must ensure that you do not create different users with the same CN or sAMAccountName as previously deleted users. Otherwise, those users will have access to the previously deleted users’ cloud application data.

Users No Longer See Private Appmarks

Issue: Users were previously able to see and access private appmarks, but they are no longer able to do so. The only change in the environment is that you are now using the filters for the connector for an LDAP identity source to reduce the search scope for importing users.

Solution: The product is working as designed. CloudAccess imports users based only on the original CN of the users. By using the filters, you are changing the search scope for the users.

If users are no longer in the search scope (as defined by the search filter), but the users exist internally in CloudAccess, those users see only public appmarks when they authenticate. The reason is that you can allow unmapped users to authenticate, but when users are outside of the search scope, CloudAccess removes the entitlements for the private appmarks.

Active Directory LDAP Search Treats Extended Characters and Normal Characters the Same

Issue: In the customized import options of the Active Directory identity source, you create a filter for Active Directory users or groups that contain special characters. The filter returns all users and groups regardless of whether the objects contain special characters. For example, if the filter searches for groüp and you have groüp and group, CloudAccess matches on both group objects. This happens whether it is group or user objects.

Workaround: The filter search option in CloudAccess uses an `ldapsearch` against Active Directory. Active Directory ignores the special characters during an `ldapsearch`. The workaround is to create filters that do not rely on special characters.

This same filter search works properly against eDirectory.

Non-Alphanumeric Characters in the Group Description Result in Users Seeing No Appmarks

Issue: If you use non-alphanumeric characters (such as !@#$%) in a group description in Active Directory, policy mapping may appear to be successful, but users in that group do not see the mapped appmarks.

Workaround: Remove any non-alphanumeric characters from the group description.

Cannot Change User or Group Filter and Change Naming Attribute in Same Operation

Issue: If you change the user or group filter to exclude some users from an LDAP identity source, and you change the naming attribute in the same operation, both the rename and the user filtering fail.

Workaround: Instead of performing both actions in the same operation, change the filter, wait for the sync, then change the naming attribute and wait for the sync.

Troubleshooting Policy Mapping Issues

Use the information in the following sections to troubleshoot policy mapping issues.

No Connectors Appear on the Policy Mapping Page

If the Policy Mapping page does not display the connectors for the SaaS applications, there are two possible solutions:

- Verify that the connectors are configured properly and enabled. For more information, see the appropriate sections for configuring connectors in the *CloudAccess Connectors Guide*.
- Click the **Refresh List** icon in the upper-right corner of the Policy Mapping page.

CloudAccess Does Not Reconcile Pending Approvals with Changes to Policy Mappings

Issue: CloudAccess does not reconcile pending approvals with changes to policy mappings. Users with pending approvals are granted the pending requests even if the mappings were removed after the requests were launched.

Workaround: If a policy mapping for a resource occurs by mistake, decline all the requests for that resource. If a policy mapping for a resource occurs correctly, but then the mapping is removed, simply decline all outstanding approval requests. You can often avoid this issue by verifying that the user is a member of the group before you grant approval, and by ensuring that requests are approved or denied in a timely manner.

Using Multiple Browsers or Browser Windows Can Result in Duplicate Mappings

Issue: If you simultaneously use more than one browser or browser window to map authorizations, CloudAccess does not warn you if you inadvertently do the same mapping in two different browsers. Clicking **Refresh** displays two identical mappings on the Approvals page, but only one of them is a valid mapping. If you remove one of the mappings, CloudAccess might not actually deprovision the user until you remove the authorization that is mapped to the group.

Workaround: You can avoid this issue by using only one browser when you create policy mappings. To work around this issue, on the CloudAccess Policy page, manually remove all duplicate authorization mappings from the role, then map the desired authorizations back to the role.

Troubleshooting Mobile Device Issues

Use the information in the following sections to troubleshoot mobile device issues.

Safari on Mobile Devices Cannot Access the Login Page After You Enable the Mobile Tool

If users cannot access the CloudAccess login page from the Safari browser on a mobile device after you enable the Mobile tool in the administration console, verify that they have installed the MobileAccess app on their mobile devices. This is a requirement once you have enabled the Mobile tool in the administration console.

Device Registration Issues

The user might not be able to register a mobile device if the device is connected to a network that uses HTTP proxy. The user receives the following error message: `Unable to parse metadata.` To work around this issue, the user can register the device from a different network that does not use HTTP proxy.

Troubleshooting CloudAccess Login Failures

Use the information in the following sections to troubleshoot CloudAccess login issues.

Users See a General Login Error

When a user is unable to log in to the CloudAccess appliance, the login page displays the message `Login failed, please try again`. Some causes of a login failure might not be obvious to either a user or a CloudAccess administrator, such as when multiple users have the same email address.

To help administrators determine the cause of the failure, the error message provides mouseover text containing an ID. You can download the `/var/log/tomcat7/catalina.out` log file and then search the log file for the ID provided in the error message. For more information about downloading log files, see "Using Troubleshooting Tools" on page 107.

Troubleshooting Authentications or Single Sign-On Issues

There can be multiple reasons why authentications to the SaaS applications (Google Apps, Salesforce, and Office 365) fail.

Time Synchronization: CloudAccess depends on timestamps to function correctly. Synchronize time between the VMware or Hyper-V host server, the appliance, and the workstations. Download the authentication or single sign-on logs. In the `catalina.out` file, search for the error `clock skew`.

SAML Authentications: Firefox contains a SAML debug add-on you can use to view the SAML authentication between CloudAccess and the SaaS applications. Download the add-on SAML tracer (https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/) to view the SAML request.

Master Node Down: If the master node is not running, users who already have accounts can log in to SaaS applications, but CloudAccess cannot provision new users. So, if new users attempt to log in to SaaS applications and receive an error indicating they should contact their system administrator, verify that the master node is running.

Troubleshooting Connector Issues

For information about viewing the current health status of a connector, see "Applications" on page 112.

For information about accessing log files for connectors, see Table 16-1, "Troubleshooting Log Files," on page 108.

For information about troubleshooting a specific connector, see the connector's information in the *CloudAccess Connectors Guide*.

Troubleshooting JDBC Identity Source Issues

Use the following information to help you troubleshoot issues with your JDBC identity source.

Issue: I have copied all of my users into the `indirect.usr` table, and the **user count** on my appliance Admin page has increased, but my users cannot log in. The **user count** never reconciles to the same number.

I also see one of the following messages in the `catalina.out` file: `mssqljdbc count: 20`, or `oraclejdbc count: 20`.

Answer: The connector for JDBC uses triggered publications, meaning the connector caches the users in the indirect.usr table only if some event (insert, update, delete) has occurred on the indirect.usr table entry, so the built-in triggers add the rows to the indirect.indirect_process table for the connector to consume and process.

To trigger a synchronization of the existing users in the indirect.usr table, you must perform a trigger action. For example, run an SQL query that would touch the records and trigger an update.

```
UPDATE indirect.usr SET disabled = disabled WHERE idu IS NOT NULL
```

Issue: I have groups defined in my indirect.grp table, but the users are not being imported to my appliance.

Answer: The connector for JDBC uses triggered publications, meaning the connector will cache the users and groups in the indirect.usr or indirect.grp table only if some event (insert, update, delete) has occurred on the table entry, so the built-in triggers add the rows to the indirect.indirect_process table for the connector to consume and process.

To trigger a synchronization of the existing users in the indirect.usr table, you must perform a trigger action. For example, run an SQL query that would touch the records and trigger an update. For example:

```
UPDATE indirect.usr SET disabled = disabled WHERE idu IS NOT NULL
```

For groups, a query similar to the one below will trigger group events:

```
UPDATE indirect.grp SET group_name = group_name
```

Issue: I have changed the indirec.proc_authuser stored procedure to use my desired tables for authentication, but I am still getting a login failure.

Answer: There are two separate ways that the stored procedure verifies the user name and password parameters passed to the proc_authuser stored procedure.

- **Oracle:** The password parameter is hashed and then compared to the existing password with the default settings.
- **MSSQL:** The stored procedure uses the PWDCOMPARE built-in function with the default settings.

In some cases, when customizing the stored procedure, the password might not be encrypted. In cases like this, the password= clause in the stored procedure might also need to be altered.

A Performing Advanced Branding

CloudAccess allows you to customize user-facing pages, such as the login page, so users see your company branding instead of the default branding.

IMPORTANT: Performing advanced branding customization requires advanced JavaServer Pages (JSP) knowledge. Before you make any changes, ensure that you have a good snapshot of your appliance that you can revert to if necessary. If you upload a bad branding file and are unable to log in to the administration console, you can re-run the appliance initialization to restore the default login pages. For more information, see “Initializing the Appliance” on page 23.

The brandable code is contained in a set of JSP files in the `/osp/jsp` directory.

To change the standard header or footer:

Edit the HTML formatting in one or both of the following files: `inc_common_body_top.jsp` or `inc_common_body_bottom.jsp`. The Java variables that the `inc_*.jsp` requires are listed at the top of the `inc_*.jsp` file. Much of this work can be done using the **Basic Customization** feature in the CloudAccess administration console. For more information, see “Customizing Branding on User-Facing Pages” on page 101.

To change the body (the space between the header and footer) of a page:

Each login, logout, and landing page contains the HTML formatting code that draws the “body” of its respective page. To customize this section of the page, you can edit the HTML formatting located between the include statements for the header and footer.

NOTE: The NetIQ logo at the bottom of the landing page cannot be removed or rebranded.

//Shared Include Files

inc_common_imports.jsp

Included in all non-shared JSPs in the Java imports area. Contains all shared import statements.

inc_common_java.jsp

Included in all non-shared JSPs in the Java code area. Contains the main Java code that processes request parameters and gathers data into standard Java variables that are used by the shared JSPs.

inc_common_head.jsp

Included in all non-shared JSPs in the JavaScript `<script>` area. Contains shared JavaScript functions that are used by the shared JSPs.

inc_common_body_top.jsp

Included in all non-shared JSPs at the top of the HTML `<body>` area. Contains the HTML formatting that creates the header for all non-shared pages. The header generally contains the product logo and name.

inc_common_body_bottom.jsp

Included in all non-shared JSPs at the bottom of the HTML `<body>` area. Contains the HTML formatting that creates the footer for all non-shared pages. The footer generally contains the NetIQ logo and a “demo version expired” warning, if applicable.

inc_common_locale.jsp

Included in the `loginselect.jsp` file in the Java code area. Contains Java code that sets the “temporary locale” form data items.

inc_common_usermessages.jsp

Included in all non-shared JSPs in the middle of the HTML `<body>` area. Contains the HTML formatting that creates the user error message section for all non-shared pages.

//Standard Login Page

loginselect.jsp

Contains the standard name-password form-based authentication page. All configurations of this page follow the standard header, body, and footer convention where the header and footer are defined in shared `inc_*.jsp` files. There are several optional objects on this page: radius login, recaptcha, and authentication contract selection.

//Second Factor Authentication Login Pages

logintotp.jsp

Contains the standard Timed One Time Password (TOTP) form-based authentication page.

fidoregister.jsp

Contains the standard Fast Identification Online (FIDO) form-based registration page.

fidologin.jsp

Contains the standard Fast Identification Online (FIDO) form-based authentication page.

//Landing Page (Home Page after Login)

landingpage_select.jsp

Contains the standard home page where users can select appmarks.

//Logout Page

landingpage_loggedout.jsp

Contains the “successful logout” page where the user is asked to close the browser to complete the logout.