

ISE with NGS Guest Accounts

By: Eric Eddy

Network Consulting Engineer

Global Security Services

Add NGS as a Token Server

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, there are menu items for "Home", "Operations", "Policy", and "Administration". A secondary navigation bar contains icons for "System", "Identity Management", "Network Resources", "Web Portal Management", and "Feed Service". The main content area is divided into two sections: "External Identity Sources" on the left and "RADIUS Token Identity Sources" on the right.

The "External Identity Sources" section on the left contains a list of categories: Certificate Authentication Profile, Active Directory, LDAP, RADIUS Token (highlighted), and RSA SecurID. The "RADIUS Token Identity Sources" section on the right features a toolbar with "Edit", "+ Add", "Duplicate", and "Delete" buttons. Below the toolbar is a table with two columns: "Name" and "Description". The table contains one entry: "NGS" with a description of "Test NGS server". The "+ Add" button in the toolbar is circled in red.

| Name | Description |
|---|-----------------|
| <input checked="" type="checkbox"/> NGS | Test NGS server |

Name the Token Server

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, there are tabs for "System", "Identity Management", "Network Resources", "Web Portal Management", and "Feed Service". The "Identity Management" tab is active, and the "External Identity Sources" sub-tab is selected. The main content area is titled "RADIUS Token Identity Sources" and has four sub-tabs: "General", "Connection", "Authentication", and "Authorization". The "General" tab is active, showing a form with the following fields:

- * Name:
- Description:

At the bottom of the form, there are "Save" and "Reset" buttons. The left sidebar shows a list of "External Identity Sources" including Certificate Authentication Profile, Active Directory, LDAP, RADIUS Token (highlighted), and RSA SecurID.

Update the Connection Details

The screenshot displays the Cisco Identity Services Engine (ISE) administration interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, there are tabs for "System", "Identity Management", "Network Resources", "Web Portal Management", and "Feed Service". The "Identity Management" tab is active, and the "External Identity Sources" sub-tab is selected. The main content area is titled "RADIUS Token Identity Sources" and has four tabs: "General", "Connection", "Authentication", and "Authorization". The "Connection" tab is currently selected. The configuration is organized into sections: "Server Connection", "Primary Server", and "Secondary Server".

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token**
- RSA SecurID

RADIUS Token Identity Sources

General | **Connection** | Authentication | Authorization

Server Connection

- Safeword Server
- Enable Secondary Server
- Always Access Primary Server First
- Failback to Primary Server after Minutes (0-99)

Primary Server

- * Host IP:
- * Shared Secret:
- * Authentication Port:
- * Server Timeout: Seconds
- * Connection Attempts:

Secondary Server

- Host IP:
- Shared Secret:
- Authentication Port:
- Server Timeout: seconds
- Connection Attempts:

The Authentication Settings – leave Defaults

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The left sidebar shows the 'External Identity Sources' menu with options like Certificate Authentication Profile, Active Directory, LDAP, RADIUS Token (selected), and RSA SecurID. The main content area is titled 'RADIUS Token Identity Sources' and has tabs for 'General', 'Connection', 'Authentication', and 'Authorization'. The 'Authentication' tab is active, showing a text box with the instruction: 'This Identity Store does not differentiate between 'authentication failed' and 'user not found' when an authentication attempt is rejected. From the options below, select how such an authentication reject from the Identity Store should be interpreted for Identity Policy processing and reporting.' Below this are two radio button options: 'Treat Rejects as 'authentication failed'' (selected) and 'Treat Rejects as 'user not found''. A note states: 'During an authentication session, initial request packets may not contain a password. The password must be requested. The prompt is configured here'. A text input field for '* Prompt' contains the text 'Password:'. At the bottom, there are 'Submit' and 'Cancel' buttons.

The Authorization Settings – leave Defaults

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The left sidebar shows 'External Identity Sources' with options like Certificate Authentication Profile, Active Directory, LDAP, RADIUS Token, and RSA SecurID. The main content area is titled 'RADIUS Token Identity Sources' and has tabs for 'General', 'Connection', 'Authentication', and 'Authorization'. The 'Authorization' tab is active, showing instructions on how to configure the RADIUS Token server to return a value in a Cisco av-pair format. A text input field labeled '* Attribute Name:' contains the value 'CiscoSecure-Group-Id'. At the bottom of the configuration area, there are 'Submit' and 'Cancel' buttons.

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token**
- RSA SecurID

RADIUS Token Identity Sources

General Connection Authentication **Authorization**

The RADIUS Token server may be configured to return a value in a Cisco av-pair with the format **attribute_name**. If this is received from the Token Server, it may be placed into a dictionary value for subsequent authorization policy. To enable this feature, enter a name for the RADIUS Token Dictionary attribute below.

A common case is a "CiscoSecure-Group-Id" in the Cisco av-pair, using the name **CiscoSecure-Group-Id**.

* Attribute Name:

Save Token Server Settings – Hit Submit

CISCO Identity Services Engine

Home | Operations | Policy | Administration

System | Identity Management | Network Resources | Web Portal Management | Feed Service

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token**
- RSA SecurID

RADIUS Token List > New RADIUS Token

RADIUS Token Identity Sources

General | Connection | Authentication | **Authorization**

The RADIUS Token server may be configured to return a value in a Cisco av-pair with the format: **attribute_name**. If this is received from the Token Server, it may be placed into a dictionary value for subsequent authorization policy. To enable this feature, enter a name for the RADIUS Token Dictionary attribute below.

A common case is a "CiscoSecure-Group-Id" in the Cisco av-pair, using the name **CiscoSecure-Group-Id**.

* Attribute Name:

Submit | Cancel

Create new Identity Source Sequence

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes the Cisco logo and the text 'Identity Services Engine'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', 'Web Portal Management', and 'Feed Service'. The 'Identity Management' tab is active, and within it, the 'Identity Source Sequences' sub-tab is selected. The main content area displays a table of existing identity source sequences. At the top of this table, there are action buttons: 'Edit', 'Add', 'Duplicate', and 'Delete'. The 'Add' button is highlighted with a red circle. The table has three columns: 'Name', 'Description', and 'Identity Stores'. The rows listed are 'Guest_Portal_Sequence', 'Guest_Source_Sequence_With_NGS', 'MyDevices_Portal_Sequence', and 'Sponsor_Portal_Sequence'.

| <input type="checkbox"/> | Name | Description | Identity Stores |
|--------------------------|--------------------------------|--|-----------------------------|
| <input type="checkbox"/> | Guest_Portal_Sequence | A built-in Identity Sequence for the Guest Portal | Internal Users, Guest Users |
| <input type="checkbox"/> | Guest_Source_Sequence_With_NGS | | Guest Users, NGS |
| <input type="checkbox"/> | MyDevices_Portal_Sequence | A built-in Identity Sequence for the My Devices Portal | Internal Users |
| <input type="checkbox"/> | Sponsor_Portal_Sequence | A built-in Identity Sequence for the Sponsor Portal | Internal Users |

Name the Sequence and Save it

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb trail is: Identity Source Sequences List > Guest_Source_Sequence_With_NGS. The page title is "Identity Source Sequence".

Identity Source Sequence

- * Name:** Guest_Source_Sequence_With_
- Description:** (Empty text area)

Certificate Based Authentication

- Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

| Available | | Selected |
|--------------------|----|-------------|
| Internal Endpoints | > | Guest Users |
| Internal Users | < | NGS |
| Maokin-AD | >> | |
| | << | |

Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Buttons: Save, Reset

Create a New Guest Portal

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The main navigation area shows 'System', 'Identity Management', 'Network Resources', 'Web Portal Management', and 'Feed Service'. The 'Settings' tab is active, and the 'Multi-Portal Configurations' page is displayed. The 'Add' button is highlighted with a red circle.

Settings

- General
- Sponsor
- My Devices
- Guest
 - Details Policy
 - Guest Roles Configuration
 - Language Template
 - Multi-Portal Configurations
 - DefaultGuestPortal
 - Deny_Access
 - NGS_Test
 - Portal Policy
 - Password Policy
- Time Profiles
- Username Policy

Multi-Portal Configurations

✎ Edit **+** Add ✕ Delete

| <input type="checkbox"/> | Multi-Portal Name | Portal Type | Description |
|--------------------------|--------------------|---------------|----------------|
| <input type="checkbox"/> | DefaultGuestPortal | Default | default portal |
| <input type="checkbox"/> | Deny_Access | CustomDefault | |
| <input type="checkbox"/> | NGS_Test | Default | |

New Portal Operations Tab

The screenshot displays the Cisco Identity Services Engine Administration interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, there are tabs for "Home", "Operations", "Policy", and "Administration". A secondary navigation bar contains icons and labels for "System", "Identity Management", "Network Resources", "Web Portal Management", and "Feed Service". A third bar shows "Sponsor Group Policy", "Sponsor Groups", and "Settings".

The main content area is titled "Settings" and features a left-hand navigation tree with categories like "General", "Sponsor", "My Devices", and "Guest". Under "Guest", there are sub-items such as "Details Policy", "Guest Roles Configuration", "Language Template", and "Multi-Portal Configurations". The "Multi-Portal Configurations" item is selected, leading to the "Multi-Portal Configuration List > New Multi-Portal Configuration" page.

The "Multi-Portal" configuration page has four tabs: "General", "Operations", "Customization", and "Authentication". The "Operations" tab is active. The "Guest Portal Policy Configuration" section includes the following options:

- Guest users should agree to an acceptable use policy
 - Not Used
 - First Login
 - Every Login
- Enable Self-Provisioning Flow
- Enable Mobile Portal
- Allow guest users to change password
- Require guest users to change password at expiration and first login
- Guest users should download the posture client
- Guest users should be allowed to do self service
 - Send self-registration credentials to whitelisted email domains

Below these options is a text input field labeled "Allowed Email Domains:" and two buttons: "Submit" and "Cancel".

New Portal Customization – Leave Defaults

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, there are tabs for "Home", "Operations", "Policy", and "Administration". The "Administration" tab is active, and the "Web Portal Management" sub-tab is selected. The main content area is titled "Multi-Portal Configuration List > New Multi-Portal Configuration". The "Multi-Portal" section has four tabs: "General", "Operations", "Customization", and "Authentication". The "Customization" tab is selected, showing the following settings:

- Language template: English (dropdown menu)
- Use browser locale:

At the bottom of the configuration area, there are "Submit" and "Cancel" buttons. The left sidebar shows the "Settings" menu with the following items:

- General
- Sponsor
- My Devices
- Guest
 - Details Policy
 - Guest Roles Configuration
 - Language Template
 - Multi-Portal Configurations (selected)
 - DefaultGuestPortal
 - Deny_Access
 - NGS_Test
 - Portal Policy
 - Password Policy
- Time Profiles
- Username Policy

New Portal Authentication

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, there are tabs for "Home", "Operations", "Policy", and "Administration". A secondary navigation bar contains icons for "System", "Identity Management", "Network Resources", "Web Portal Management", and "Feed Service". The "Settings" tab is currently selected.

The left sidebar shows a tree view of settings categories: "General", "Sponsor", "My Devices", "Guest", "Language Template", "Multi-Portal Configurations", "Time Profiles", and "Username Policy". The "Multi-Portal Configurations" category is expanded, showing sub-items like "DefaultGuestPortal", "Deny_Access", "NGS_Test", "Portal Policy", and "Password Policy".

The main content area is titled "Multi-Portal Configuration List > New Multi-Portal Configuration". It features a "Multi-Portal" section with four tabs: "General", "Operations", "Customization", and "Authentication". The "Authentication" tab is active. A configuration field labeled "* Identity Store Sequence" has a dropdown menu with the selected value "Source_Sequence_With_NGS". At the bottom of the configuration area, there are "Submit" and "Cancel" buttons.

Create new Authorization Profile

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and menu items for Home, Operations, Policy, and Administration. Below this, there are tabs for Policy Sets, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The main content area is titled "Authorization Profiles > New Authorization Profile".

Authorization Profile Configuration:

- * Name:** NGS-CWA
- Description:** (empty text field)
- * Access Type:** ACCESS_ACCEPT
- Service Template:**

Common Tasks:

- VLAN
- Voice Domain Permission
- Web Redirection (CWA, DRW, MDM, NSP, CPP)

Web Redirection Settings:

- Centralized Web Auth:
- ACL: ACL-WEBAUTH-REDIRECT
- Redirect:
- Value: NGS_Test

Advanced Attributes Settings:

Select an item = - +

Attributes Details:

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL-WEBAUTH-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&portal=NGS_Test&action=cwa
```

Buttons:

ISE Authentication

| | | | | |
|-------------------------------------|---------|---------------------------------------|--------------------------------------|-----|
| <input checked="" type="checkbox"/> | MAB | : If Wireless_MAB OR Wired_MAB | Allow Protocols : MAB_Authentication | and |
| <input checked="" type="checkbox"/> | Default | : use Internal Endpoints | | |

ISE Authorization

| | | | | |
|---|-----|-------------------------------|---|-------------------|
| ☰ | ✓ | Guest Access Internal Account | if (Guest OR ActivatedGuest) AND Network Access:UseCase EQUALS Guest Flow | then PermitAccess |
| ☰ | ✓ | Guest Access NGS Accounts | if (Network Access:AuthenticationIdentityStore EQUALS NGS AND Network Access:UseCase EQUALS Guest Flow) | then PermitAccess |
| ☰ | ✎ ✓ | CWA | if Network Access:AuthenticationMethod EQUALS Lookup | then NGS-CWA |

On NGS Add ISE PSNs as a RADIUS Client

The screenshot displays the Cisco NAC Guest Server Administration web interface. The left sidebar contains a navigation menu with the following items: Authentication, Guest Policy, Devices (expanded), NAC Appliances, RADIUS Clients (highlighted), Email Settings, SMS Settings, Syslog Monitoring, User Interface, Hotspot, and Server. The main content area is titled 'Add RADIUS Client' and contains the following fields and controls:

- Name:** ise-psn
- IP Address:** 192.168.0.44
- Secret:** [masked] **Confirm:** [masked]
- Description:** ISE PSN
- Device sends Calling Station IP:**
- Attribute:** [text input] **Add** button
- Value:** [text input]
- Buttons:** Move up, Remove, Move down

At the bottom of the form are two buttons: 'Add RADIUS Client' and 'Cancel'.

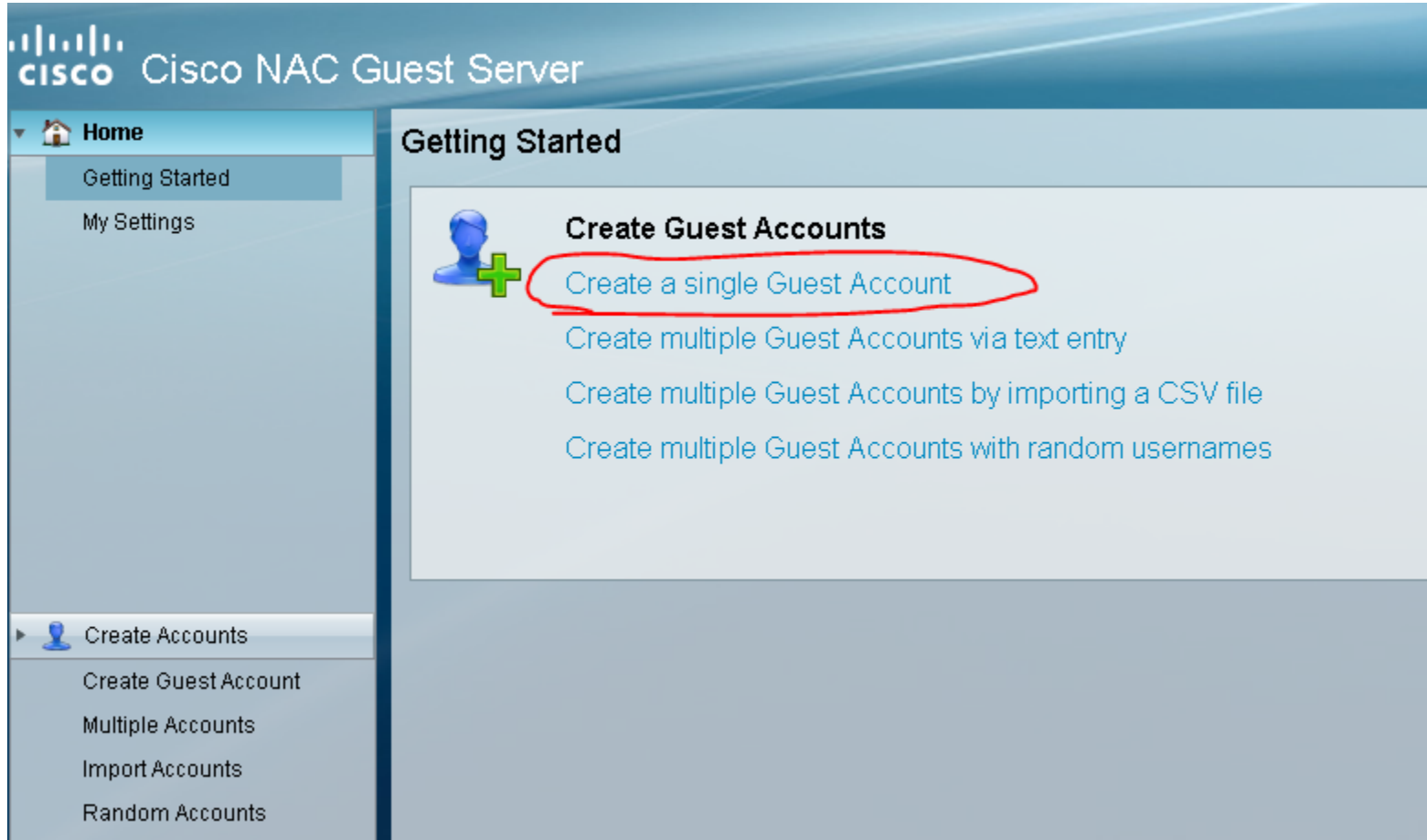
Restart the RADIUS Process To apply the Changes

The screenshot shows the Cisco NAC Guest Server Administration interface. The left sidebar contains a navigation menu with the following items: Authentication, Guest Policy, Devices (expanded), NAC Appliances, RADIUS Clients (selected), Email Settings, SMS Settings, Syslog Monitoring, User Interface, Hotspot, and Server. The main content area is titled "Edit RADIUS Client" and features a table with two entries:

| Name | IP Address | Description | |
|---------------------------|--------------|----------------|--|
| ise-psn-1 | 192.168.0.44 | ISE home PSN 1 | |
| ise-psn-2 | 192.168.0.45 | ISE Home PSN 2 | |

Below the table is an "Add RADIUS Client" button. A text instruction reads: "If any changes are made to the radius clients please click the Restart RADIUS button to apply them." The "Restart" button is circled in red. Below this is another instruction: "To activate RADIUS debug mode click the Debug button. To turn debug mode off, click the restart button." The "Debug" button is also visible.

Create a Guest Account



The screenshot displays the Cisco NAC Guest Server web interface. The top navigation bar includes the Cisco logo and the text "Cisco NAC Guest Server". A left-hand sidebar menu is visible, with "Home" expanded to show "Getting Started" and "My Settings". Below this, "Create Accounts" is expanded to show "Create Guest Account", "Multiple Accounts", "Import Accounts", and "Random Accounts". The main content area is titled "Getting Started" and features a "Create Guest Accounts" section. This section includes a blue person icon with a green plus sign. The first option, "Create a single Guest Account", is circled in red. Other options listed are "Create multiple Guest Accounts via text entry", "Create multiple Guest Accounts by importing a CSV file", and "Create multiple Guest Accounts with random usernames".

Getting Started

Create Guest Accounts

- Create a single Guest Account
- Create multiple Guest Accounts via text entry
- Create multiple Guest Accounts by importing a CSV file
- Create multiple Guest Accounts with random usernames

And you are Done!

Guest accounts should now work on the ISE Hosted guest portal.

Thank you.

