

---

## Upgrading from IVE OS version 3.x to 4.0

NetScreen Instant Virtual Extranet OS version 4.0 introduces the next-generation secure remote access appliance with a new Access Management system that supports flexible and dynamic authentication and authorization policies. This document provides a brief overview of the 4.0 Access Management system and describes how 3.x system data migrates to this system. Before upgrading from a 3.x OS, please review this document, the 4.0 release notes, and the *Administration Guide* PDF available on the support site: support.netscreen.com. If you have additional questions, please contact the NetScreen Secure Access Products support team.

---

### Contents

|   |    |
|---|----|
| 4.0 Access Management Conceptual Overview .....               | 3  |
| Comparing 3.x and 4.0 authentication and authorization .....  | 4  |
| Changes to authentication servers .....                       | 5  |
| 3.x Authentication Server Definition .....                    | 6  |
| 4.0 Authentication Realm .....                                | 6  |
| 3.x Authentication Server Migration Path .....                | 6  |
| 3.x Group Mapping Rules Migration Path .....                  | 8  |
| Additional Information for LDAP Servers .....                 | 11 |
| LDAP Authentication Server Migration .....                    | 11 |
| LDAP Group Lookup Server Migration .....                      | 12 |
| Changes to authorization groups .....                         | 13 |
| 3.x Authorization Group Definition .....                      | 14 |
| 4.0 User roles .....  | 15 |
| 4.0 Resource policies .....                                   | 16 |
| 3.x Authorization Group Migration Path .....                  | 17 |
| Specific Resource Policy Details .....                        | 18 |
| Miscellaneous Upgrade Details .....                           | 21 |
| Upgrade Summary .....   | 23 |
| Reference A: Authentication and Authorization Flowchart ..... | 24 |
| Reference B: User Interface Mapping—3.x to 4.0 .....          | 27 |



---

## 4.0 Access Management Conceptual Overview

IVE 4.0 enables you to secure your company resources based on authentication policies, user profile information, and resource policies. These three levels of control enable you to administer the appropriate access management for your extended enterprise. You can specify security requirements that users must meet to sign in to the IVE, to gain access to IVE features, and even to access specific URLs, files, and other server resources. The IVE enforces the policies, rules and restrictions, and conditions you configure to prevent users from connecting to or downloading unauthorized resources and content.

Resource accessibility begins with the authentication realm. An **authentication realm** is a grouping of authentication resources, including an authentication server, authentication policy, directory server (optional), and role mapping rules. One or more authentication realms are associated with an IVE sign-in page. When more than one realm exists for a sign-in page, a user must specify a realm before submitting her credentials. When the user submits her credentials, the IVE checks the authentication policy defined for the chosen realm. The user must meet the security requirements you define for a realm's authentication policy or else the IVE does not forward the user's credentials to the authentication server.

At the realm level, you can specify security requirements based on the user's source IP, the browser from which the user accesses the IVE, the user's possession of a client-side certificate, the length of the user's password, whether or not Host Checker is either installed or enforcing policies on the user's machine, or whether or not Cache Cleaner is either installed or running on the user's machine. If the user meets the requirements specified by the realm's authentication policy, then the IVE forwards the user's credentials to the appropriate authentication server. If this server successfully authenticates the user, then the IVE evaluates the role mapping rules defined for the realm to determine which roles to assign to the user.

A **role** is a defined entity that specifies IVE session properties for users who are mapped to the role. These session properties include information such as session timeouts, bookmarks, and enabled Access features—Web browsing, file browsing, Secure Application Manager, Network Connect, Telnet/SSH, Secure Meeting, and Email Client. A role's configuration serves as the second level of resource access control. Not only does a role specify the access mechanisms available to a user, but you can also specify restrictions with which users must comply *before* they are mapped to a role. The user must meet these security requirements or else the IVE does not map the user to a role.

At the role level, you can specify security requirements based on the user's source IP, browser, and possession of a client-side certificate, as well as whether or not Host Checker is either installed or enforcing specified policies on the user's machine or whether or not Cache Cleaner is running on the user's machine. If the user meets the requirements specified either by a role mapping rule or a role's restrictions<sup>1</sup>, then the IVE maps the user to the role. When a user makes a request to the backend resources available to the role, the IVE evaluates the corresponding Access feature resource policies.

A **resource policy** is a set of resource names (such as URLs, hostnames, and IP address/netmask combinations) to which you grant or deny access or other resource-specific actions, such as rewriting and caching. A resource policy serves as the third level of resource access control. While a role may grant access to certain types of features and resources (such as bookmarks and applications), whether or not a user can access a specific resource, is controlled by resource policies. These policies may even specify conditions that, if met, either deny or grant user access to a server share or file. These conditions may be based on security requirements that you specify. The user must meet these security requirements or else the IVE does not process the user's request.

At the resource level, you can specify security requirements based on the user's source IP, browser, possession of a client-side certificate, the request's time-of-day, whether or not Host Checker is either installed or enforcing policies on the user's machine, or whether or not Cache Cleaner is either installed or running on the user's machine. If the user meets the requirements specified by a resource policy's conditions, then the IVE either denies or grants access to the requested resource. You may enable Web access at the role level, for example, and a user mapped to the role may make a Web request. You may

---

<sup>1</sup> You may specify security requirements for a role in two places—in the role mapping rules of an authentication realm (using custom expressions) or by defining restrictions in the role definition. The IVE evaluates the requirements specified in both areas to make sure the user complies before it maps the user to a role.

also configure a Web resource policy to deny requests to a particular URL or path when Host Checker finds an unacceptable file on the user’s machine. In this scenario, the IVE checks to see if Host Checker is running and indicates that the user’s machine complies with the required Host Checker policy. If the user’s machine complies, meaning the unacceptable file is not found, then the IVE grants the user access to the requested Web resource.

## Comparing 3.x and 4.0 authentication and authorization

In IVE version 3.x, the AA process for authorizing users consists of three main steps:

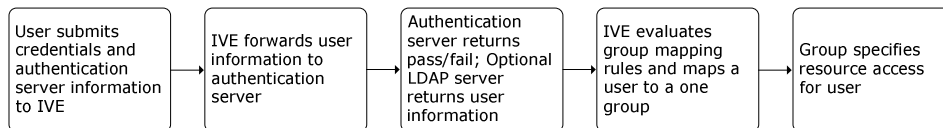
- A user signs in to the IVE and the IVE forwards the user’s credentials to the specified authentication server.
- The IVE either receives authorization group information as part of the authentication transaction (from a RADIUS or an LDAP server) or retrieves a user’s profile (attribute and group information) from an LDAP server after performing the authentication transaction.
- The IVE evaluates the group mapping rules and displays all matching groups to the user. The user then selects the group to join for that session. (If the user maps to only one group, then the IVE automatically maps the user to that group.)

In IVE version 4.0, the AA process for authorizing users consists of four main steps:

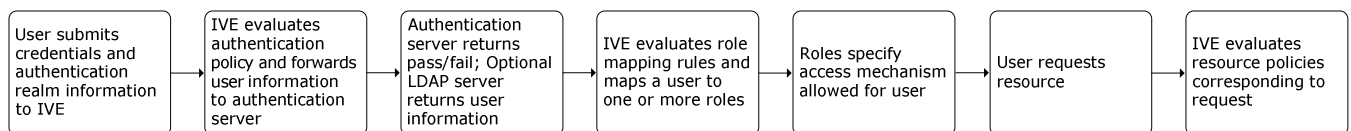
- A user signs in to the IVE, and if the user complies with the realm’s authentication policy, the IVE forwards the user’s credentials to the specified authentication realm.
- The IVE either receives authorization group information as part of the authentication transaction (from a RADIUS or an LDAP server) or retrieves a user’s profile (attribute and group information) from an LDAP server after performing the authentication transaction.
- The IVE evaluates the role mapping rules, and if the user meets the specified requirements, the IVE maps the user to one or more roles, which define the resources available to the user at a high level (such as Web access, file access, or network access). The IVE merges the permissions from all valid roles (if configured to do so) so that the user may access all permitted resources specified by each role.
- The user makes a resource request, and the IVE evaluates the resource policies corresponding to the user’s request to determine if the resource is available to the user.

The following figure summarizes the AA steps involved in providing user resource access in IVE version 3.x and 4.0. For a detailed flowchart of the transactions between a user, the IVE, and an authentication server, see “Authentication and Authorization Flowchart” on page 24.

### 3.0 AA process



### 4.0 AA process



This figure shows the transactions that occur in IVE versions 3.0 and 4.0 during the authentication and authorization (AA) process of Access Management.

IVE version 4.0 introduces a new authentication and authorization (AA) process for authenticating and authorizing users. After upgrading from IVE version 2.x or 3.x (legacy or standard mode), the Administrator Console displays a new menu that reflects the 4.0 AA process. This section compares the 4.0 interface to that of a 3.x (standard mode) Administrator Console. If you are upgrading from version 2.x or 3.x running in legacy mode, please consult “Upgrading from IVE version 2.x to 3.x” posted on the Support Site under “Product Documentation > Release 2.x” to understand the relationship of the 2.x Administrator Console to that in version 3.x.

Also, note that:

- If you are upgrading an existing IVE 2.x configuration or 3.x configuration running in legacy mode to a 4.0 service package, the upgrade process automatically converts your data first to the standard 3.0 AA data structure and then to the 4.0 AA data structure. This two-step conversion process:  
Eliminates the need for you to migrate 2.x or 3.x legacy mode data to the standard mode of IVE version 3.0 before upgrading to a 4.0 service package. Please see “Considerations When Upgrading IVE version 2.x to 3.0” posted on the Support Site under “Product Documentation > Release 2.x” to understand the what happens to 2.x or 3.x legacy mode user data.
- If you are upgrading an existing IVE 3.x configuration running in standard mode to a 4.0 service package, the upgrade process automatically converts your data to the 4.0 AA data structure in one step.

**Important:**

The IVE stores two system configurations at one time—the current version and the previous version. Each time you wish to install a newer beta service package, we *strongly recommend* that you perform a system rollback first. The rollback process enables you to restore your original 2.x or 3.x configuration before testing the latest 4.0 beta service package.

If you do not perform a system rollback before installing another service package, the current configuration (in this case, the first 4.0 service package you installed) overwrites your original 2.x/3.x configuration and becomes the “previous” package version to the newly installed package, which is the “current” version. In this scenario, you cannot return to your original configuration unless you 1) perform a factory reset, 2) upgrade to the appropriate 2.x or 3.x service package, and then 3) import previously saved system, user, ACL (access control list), and bookmark data.

## Changes to authentication servers

Just like in IVE version 3.x, the authentication process in version 4.0 requires administrators to define servers against which user credentials are authenticated. In 4.0, however, the authentication server used to authenticate a user is part of a larger entity—an authentication realm, which also includes an authentication policy, an (optional) directory server, and role mapping rules. When you upgrade from version 3.x, each 3.x authentication server definition is converted to an authentication realm. This section summarizes a 3.x authentication server definition and describes a 4.0 authentication realm to provide context for how a 3.x configuration migrates to version 4.0. The function of an authentication realm is described in more detail in the *Administration Guide* PDF<sup>2</sup>.

---

<sup>2</sup> The *Administration Guide* content is also available in HTML format from the Web console (previously called the Administrator Console) Help link.

---

## 3.x Authentication Server Definition

A 3.x authentication server definition<sup>3</sup> specifies this information:

- **The server's settings**, such as its name, port, and IP address, as well as any information needed to talk to the server, such as protocol or password information, and in the case of LDAP, DN information. This information is specified on the 3.x Authentication & Authorization > Authentication Servers > ServerName > Settings tab.
- **Authorization group settings**, which specify *how* to map users authenticated by the server to an IVE authorization group, such as by attribute (returned by RADIUS or LDAP), by query response (using LDAP), by username, or by group assignment. If the setting is to map a user based on a query response from LDAP, then the authentication server definition also contains group lookup server information. The authorization group settings are specified on the Authentication & Authorization > Authentication Servers > ServerName > Settings tab (in the Authorization Group Settings section). Note that group lookup server information is specified by clicking the Define button on this tab.
- **Group mapping rules**, which specify *who* (identified by attribute, user/group information, or username) to map to a particular IVE authorization group. These rules are specified on the Authentication & Authorization > Authentication Servers > ServerName > Group Mapping tab.

A 3.x IVE Local Authentication server also contains local user records and may contain "user admins," who are users in the IVE Local Authentication database who are given limited administrative capabilities.

## 4.0 Authentication Realm

An **authentication realm** is a grouping of authentication resources, including:

- **An authentication server**, which verifies that the user is who he claims to be. The IVE forwards credentials that a user submits on a sign-in page to an authentication server.
- **An authentication policy**, which specifies realm security requirements that need to be met before the IVE submits a user's credentials to an authentication server for verification.
- **A directory server**, which is an LDAP server that provides user and group information to the IVE that the IVE uses to map users to one or more user roles.
- **Role mapping rules**, which are conditions a user must meet in order for the IVE to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

When comparing a 4.0 authentication realm to a 3.x authentication server definition, you can see that a realm provides greater control over who may attempt to sign in to your IVE and more flexibility in specifying how servers are used throughout your system.

## 3.x Authentication Server Migration Path

In 3.x, you configure a server definition in one place—on the Authentication & Authorization > Authentication Servers page. In 4.0, you configure realm components in two places:

- You specify authentication servers and directory servers<sup>4</sup> on the System > Signing In > Servers page.
- You specify the realm name, authentication policy, and role mapping rules on either the Administrators > Authentication page or Users > Authentication page.

---

<sup>3</sup> In version 3.x documentation, an authentication server definition is also referred to as an "instance."

<sup>4</sup> In version 3.x, a server that provides user information for authorization purposes is called an "authorization server." In 4.0, a server used for this purpose is called a "directory server."

Note: 4.0 servers (authentication and directory) are resources shared by both administrator and user realms. For ease of server administration, you configure them in a single location (separate from the other realm components). When you specify a server for a realm, you simply need to point to the server you want to use for authentication or authorization. Because you configure servers separately from a realm, you only need to specify the server configuration one time<sup>5</sup> and then can point to it for any number of realms; in 3.x, you must configure two server definitions if you want to use the same server for both authentication and authorization.

When you upgrade a 3.x configuration to 4.0, therefore, the information contained in each 3.x server definition is split between the 4.0 System > Signing In > Servers page and either the Administrators > Authentication page or the Users > Authentication page. Specifically, for every 3.x server definition, the upgrade process creates:

- **A 4.0 authentication server definition**

The IVE uses the 3.x server name to name the 4.0 server. For example, if the 3.x authentication server name is "employees-hq," then the IVE creates a 4.0 authentication server on the System > Signing In > Servers page called "employees-hq."

- **A 4.0 directory server definition** (only if the 3.x server definition defined a group lookup server)

The IVE uses the 3.x server name prefaced by "authorization\_" to name the 4.0 directory server. For example, if the 3.x authentication server name is "employees-hq" and a secondary group lookup server is specified as part of the server definition, then the IVE creates a 4.0 directory server on the System > Signing In > Servers page called "authorization\_employees-hq."

- **A 4.0 user authentication realm**

The IVE uses the 3.x server name to name the 4.0 authentication realm. For example, if the 3.x authentication server name is "employees-hq," then the IVE creates a 4.0 authentication realm on the Users > Authentication page called "employees-hq."

On the 4.0 Users > Authentication page, you click on a realm to access and configure its settings, which are divided among three tabs:

- **General** tab, which contains:
  - The realm name and optional description (none exists for migrated server definitions).
  - A **Servers** section that enables you to select the authentication server and optional directory server to use when authenticating users who specify the realm on the sign-in page.
  - An **Other settings** section that lists authentication policy requirements and the number of role mapping rules that exist for the realm (see the description for the Role Mapping tab below).
  - **Authentication Policy** tab, which enables you to configure six types of requirements to place on realm users when they try to access an IVE sign-in page associated with the realm. These requirements may be based on the user's source IP, browser type, client-side certificate possession and attributes, password length, and whether or not the user meets the specified Host Checker and Cache Cleaner requirements.
  - **Role Mapping** tab, which contains the migrated group mapping rules. Each 3.x group mapping rule migrates to one role mapping rule. And, if you selected the 3.x option to "map unmatched users" to a particular 3.x authorization group, then one additional 4.0 role mapping rule is created to handle this case. The 3.x option to "deny access to unmatched users" does not require a 4.0 role mapping rule equivalent; users not mapped to a role during the authentication process do not gain access to the IVE.

**Additionally during a 3.x to 4.0 upgrade:**

- Two sign-in policies are created on the 4.0 System > Signing In > Sign-in Policies tab. A **sign-in policy** is a policy that defines which sign-in page to show an administrator or user (using a built-in or custom template) and the list of realms to present to the administrator or user. By default, the upgrade process creates two sign-in policies:

<sup>5</sup> In 3.x, you can only use an LDAP server as a group lookup server. In 4.0, you may also point to a RADIUS server for group lookup information.

- One for administrators that maps an IVE URL ending in /admin to the default sign-in page for administrators.
- One for users that maps any IVE URLs for end-users to the default sign-in page for users.

After upgrading, you can specify additional URLs and sign-in pages and then map each URL to the desired sign-in page.

- When upgrading from 3.x to 4.0, the default behavior is “user must select from among assigned roles”; In 3.x, a user is presented with a *list* of matched groups from which he chooses a group for the session. After an upgrade, a user is presented with a list of matched roles from which she chooses a role for the session. You can configure an authentication realm to merge all roles to which the user is mapped, however, so that the IVE assigns the access privileges from all matched roles to the user for the session. See the *Administration Guide* PDF for more information about merging roles.

### 3.x Group Mapping Rules Migration Path

In 3.x, you may specify up to four ways in which the IVE maps users to authorization groups. The available options for each server appear in the Authorization Group Settings section on the server’s Settings tab and may include:

- **Authorization group assigned based on attribute in authentication response**—when selected, each group mapping rule on the 3.x Group Mapping tab is converted into one role mapping rule on the 4.0 Role Mapping tab.
- **Authorization group assigned based on querying a group lookup server**—when selected, each group mapping rule on the 3.x Group Mapping tab is converted into one role mapping rule on the 4.0 Role Mapping tab.
- **Authorization group assigned based on username**—when selected, each group mapping rule on the 3.x Group Mapping tab is converted into one role mapping rule on the 4.0 Role Mapping tab.
- **All users are assigned to [a specified] group**—when selected, one role mapping rule is created on the 4.0 Role Mapping tab that maps all authenticated users to the specified role (which is a group in 3.x).

The following table summarizes the 3.x user-to-group mapping options and how they are migrated to the 4.0 configuration. Note that 4.0 role mapping rules are written using the custom expression language.

| <b>3.x Authorization Group Settings Option</b><br>Authentication & Authorization > Authentication Servers > <i>ServerName</i> > Settings tab  | <b>4.0 Migration Path</b>   | <b>3.x Group Mapping Rules</b><br>Authentication & Authorization > Authentication Servers > <i>ServerName</i> > Group Mapping tab  | <b>4.0 Role Mapping Rules</b><br>Users > Authentication > <i>RealmName</i> > Role Mapping tab   |
|---|---|--|---|
| Authorization group assigned based on attribute in authentication response*<br>When using this option, the IVE maps users to authorization groups based on group information returned by RADIUS or LDAP.<br><br>This option is available only for LDAP and RADIUS servers.  | If this option is selected, then the 3.x server definition specifies group mapping rules based on the value that may be returned for either a RADIUS attribute (typically filter-id) or an LDAP attribute (typically memberOf). | <b>Rule 1:</b> These external groups<br>ou=employees-hq,o=acmegizmo.com<br><b>map to:</b> employees-hq<br><br><b>Rule 2:</b> These external groups<br>ou=partnerA,o=acmegizmo.com<br><b>map to:</b> partnerA<br><br><b>Mapping unmatched users option</b><br>Map unmatched users to: guests                                | When:<br>UserAttr.filter-id="ou=employees-hq,o=acmegizmo.com"<br><b>Assign to:</b> employees-hq<br><br>When:<br>UserAttr.filter-id="ou=partnerA,o=acmegizmo.com"<br>Assign to: partnerA<br><br>When:<br>UserAttr.filter-id is not "ou=employees-hq,o=acmegizmo.com", "ou=partnerA,o=acmegizmo.com"<br>Assign to: guests |
| Authorization group assigned based on querying a group lookup server*<br>When using this option, the IVE maps users to authorization groups based on group information returned by an LDAP server.<br><br>If you chose this option for an LDAP server, the IVE authenticates users with the server specified for the server definition and then authorizes users using the <i>additional</i> LDAP server that you define in the Configure Group Lookup Server dialog.<br><br>This option is available for all servers except the local IVE authentication server. | If this option is selected, then the 3.x server definition specifies group mapping rules based on the group names that may be returned from the group lookup server.  | <b>Rule 1:</b> These external groups<br>cn=employees-hq,ou=US Office, dc=acmegizmo,dc=com<br><b>map to:</b> employees-hq<br><br><b>Rule 2:</b> These external groups<br>cn=partnerA,ou=US Office,dc=acmegizmo,dc=com<br>map to:<br>partnerA<br><br><b>Mapping unmatched users option</b><br>Map unmatched users to: guests | When:<br>group="cn=employees-hq,ou=US Office,dc=acmegizmo,dc=com"<br><b>Assign to:</b> employees-hq<br><br>When:<br>group="cn=partnerA,ou=US Office,dc=acmegizmo,dc=com"<br>Assign to: partnerA<br><br>When:<br>group is not "ou=employees-hq,o=acmegizmo.com", "ou=partnerA,o=acmegizmo.com"<br>Assign to: guests      |

|   |  |   |  |
|---|--|---|--|
| <p>Authorization group assigned based on username*</p> <p>If you chose this option, the IVE maps users to authorization groups based on their usernames.</p> <p>This option is available for all servers.</p>                         | <p>If this option is selected, then the 3.x server definition specifies group mapping rules based on IVE usernames.</p>  | <p><b>Rule 1:</b> These usernames<br/>cay<br/>gil<br/>roz<br/><b>map to:</b> employees-hq</p> <p><b>Rule 2:</b> These usernames<br/>karen<br/>scott<br/><b>map to:</b> partnerA</p> <p><b>Mapping unmatched users option</b><br/>Map unmatched users to: guests</p>               | <p>When:<br/>username="cay", "gil", "roz"<br/><b>Assign to:</b> employees-hq</p> <p>When:<br/>username="karen", "scott"<br/>Assign to: partnerA</p> <p>When:<br/>username is not="cay", "gil", "roz", "karen", "scott"<br/>Assign to: guests</p>   |
| <p>All users are assigned to a specified authorization group*</p> <p>Choose this option if you want the IVE to map all authenticated users to the specified authorization group.</p> <p>This option is available for all servers.</p> | <p>If this option is selected, then the 3.x server definition does not have any <i>active</i> group mapping rules. (Even if you have specified rules on the 3.x Group Mapping tab, they are not used when this option is selected, because users are assigned to a specified authorization group.) Because no rules are active, the upgrade process creates one 4.0 role mapping rule to map all users to the specified user role (3.x authorization group).</p> | <p>None</p>   | <p>When:<br/>username="*"<br/><b>Assign to:</b> employees-hq</p>   |
| <p>*Map unmatched users to a specified group</p>  |  |   |  |
| <p>This option is available for all servers at the bottom of the Group Mapping tab.</p>   | <p>If this 3.x option is selected, then the upgrade process creates an additional 4.0 role mapping rule that specifies this condition:</p> <p>If a user is not covered by a previous role mapping rule in the list, then map the user to the specified user role (3.x authorization group).</p>  | <p>The "map unmatched users..." option on the 3.x Group Mapping tab may be configured for any of the four "Authorization Group Settings" options on the 3.x Settings tab (although it is inapplicable and when choosing to map all users to a specified authorization group).</p> | <p>The 4.0 role mapping rule is in the format:</p> <p>When:<br/>condition is not="value1", "value2", ...<br/><b>Assign to:</b> specifiedRole</p> <p>Where:<br/><i>condition</i> = condition used in previous rules<br/><i>valueN</i> = a value in a rule; this comma delimited list is created by concatenating the values from all the rules<br/><i>specifiedRole</i> = the 3.x authorization group</p> |

## Additional Information for LDAP Servers

In general, 3.x authentication server information specified on the 3.x Authentication & Authorization > Authentication Servers > *ServerName* > Settings tab migrates to the 4.0 System > Signing In > Servers > *ServerName* > Settings tab. In the case of an LDAP server, however, the user interface is organized slightly differently. This section describes how 3.x LDAP server information migrates to 4.0. See "LDAP Group Lookup Server Migration

" on page 12 for information about how LDAP servers used for group lookup information migrate to 4.0.

### LDAP Authentication Server Migration

3.x to 4.0 LDAP server migration summary:

- The 3.x fields that specify server settings for the LDAP server and backup servers migrate to the same place on the 4.0 server Settings tab. These fields appear above the Test Connection button in both 3.x and 4.0 and include:
  - Name
  - LDAP Server
  - LDAP Port
  - Backup LDAP Server1
  - Backup LDAP Port1
  - Backup LDAP Server2
  - Backup LDAP Port2
  - Connection \*Note that "LDAP over TLS" is in the "Bind options" section of the 4.0 Settings tab and is represented as "StartTLS bind."
  - LDAP Server Type
- The 3.x "Enable Password Management" option (above the Test Connection button in 3.x) migrates to the 4.0 realm (corresponding to the 3.x LDAP server) on the Authentication Policy > Password sub-tab<sup>6</sup>. Note that the "Enable Password Management" option appears on the 4.0 Authentication Policy > Password sub-tab only for realms that use LDAP or Active Directory servers as the authentication server.
- The 3.x "Require application authentication to search the LDAP database" option and the associated "Application DN" and "Application password" fields appear in a section called "Authentication required?" on the 4.0 Settings tab.
- The 3.x "Static Distinguished Name (DN)" option does not migrate to 4.0. If you use this option in 3.x, then the value specified in the associated "DN" field migrates to the 4.0 "Finding user entries" section as follows:
  - The first RDN migrates to the 4.0 "Filter" field
  - The second RDN migrates to the 4.0 "Base DN" field

For example, if the static DN in 3.x is "cn=<USER>,dc=sales,dc=com," then "cn=<USER>" migrates to the 4.0 "Filter" field and "dc=sales" migrates to the "Base DN" field.
- The 3.x "Dynamic Distinguished Name (DN)" option migrates directly to the 4.0 "Finding user entries" section.
- The 3.x "Authorization Group Settings" options migrate to 4.0 as described in the table on page 9. Note that if you chose "Authorization group assigned based on querying a group lookup server," then you also specified an LDAP server as the group lookup server in the 3.x Configure Group Lookup Server dialog:

---

<sup>6</sup> The Authentication Policy > Password sub-tab appears on both the Administrators > Authentication page and Users > Authentication page. During an upgrade from 3.x to 4.0, the 4.0 authentication realm created from a 3.x server appears on the Users > Authentication page. If the 3.x authentication server is an LDAP server, then the 3.x "Enable Password Management" option appears on the Authentication Policy > Password sub-tab of the corresponding realm under Users > Authentication.

## LDAP Group Lookup Server Migration

If you specified a group lookup server within a 3.x server definition<sup>7</sup>, then the corresponding 4.0 authentication realm created during the upgrade process includes a server definition (on the System > Signing In > Servers tab) for this authorization server. This server is named "authorization\_<primaryServer>," where <primaryServer> is the name of the 3.x authentication server. For example, if the 3.x authentication server is "employees-hq," then the upgrade process creates a 4.0 server called "authorization\_employees-hq." This authorization server definition uses the server settings (name, IP address, port, back-up server, and connection information) as the corresponding authentication server. The 4.0 "Finding user entries" and "Determining group membership" fields are populated with data from the 3.x group lookup server dialog.

**Figure 1 (3.x dialog):**  
Standard LDAP server configured as a group lookup server

**Figure 2 (3.x dialog):**  
iPlanet LDAP server configured as a group lookup server

The information that you specify in the Configure Group Lookup Server dialog is migrated to the 4.0 server definition (System > Signing In > Servers > authorization\_<ServerName> > Settings tab) as follows:

**For both a standard LDAP server and an iPlanet server configured as a 3.x group lookup server:**

- The "LDAP Server," "LDAP Port," and "Connection" fields in the 3.x dialog migrate to the top of the corresponding 4.0 server's Settings tab.
- The "Authentication required to search LDAP" option and the associated "Application DN" and "Password" fields in the 3.x dialog migrate to the "Authentication required?" section on the 4.0 server's Settings tab.

**For a standard LDAP server configured as a 3.x group lookup server:**

- The "Base DN" field in the 3.x dialog migrates to the 4.0 "Finding user entries—Base DN" field.
- The "Filter" field in the 3.x dialog migrates as "cn=\*" to the 4.0 "Finding user entries—Filter" field.
- The value in the "Attribute" field in the 3.x dialog migrates to the corresponding 4.0 authentication realm "Role Mapping" tab as a rule written in the format: UserAttr.<AttributeValue>=<USERDN>

**Important:** If the "Attribute" field is blank in the 3.x dialog for a standard LDAP group lookup server (Figure

<sup>7</sup> In 3.x, you specify an LDAP group lookup server by clicking the Define button on the Authentication & Authorization > Authentication Servers > <ServerName> > Settings tab.

1), iPlanet is assumed to be the authentication server as well as the authorization server. In this case, the 3.x dialog "Base DN" information migrates to the 4.0 "Determining group membership—Base DN" field; the 4.0 "Determining group membership—Filter" field is populated with `cn=<GROUPNAME>`; and the attribute name before the equal sign (=) migrates to the 4.0 "Determining group membership—Member Attribute field," such as "sAMAccountName" in Figure 1. The 4.0 "Determining group membership—Query Attribute" field is not populated with any data; IVE 3.x did not support dynamic groups.

#### For an iPlanet server configured as a 3.x group lookup server:

- The "User Filter" field in the 3.x dialog migrates to the 4.0 "Finding user entries—Filter" field.
- The "User Base DN" field in the 3.x dialog migrates to the 4.0 "Finding user entries—Base DN" field.
- The 3.x dialog "Group Filter" attribute name before the equal sign (=) migrates to the 4.0 "Determining group membership—Member Attribute field," such as "uniquemember" in Figure 2.
- The "Group Base DN" field in the 3.x dialog migrates to the 4.0 "Determining group membership—Base DN" field.
- The "Group Name Attribute" field in the 3.x dialog is converted to "cn=<GROUPNAME>" in the 4.0 "Determining group membership—Filter" field.

#### Important:

If you use the same iPlanet server for both authentication and authorization in 3.x, make sure the 3.x iPlanet server definition is configured as follows to ensure that the upgrade process creates the appropriate 4.0 authentication and directory server definitions:

1. Under "Authorization Group Settings," the 3.x iPlanet server definition must specify the option: "Authorization group assigned based on querying a group lookup server."
2. In the "Configure Group Lookup Server" dialog, the "LDAP Server Type" must specify: "Look Up Group (Standard LDAP Server)."
3. The "Attribute" field that appears in the "Configure Group Lookup Server" dialog for standard LDAP servers must be empty. If you specify an attribute in this field, then the IVE thinks it needs to query iPlanet user objects and the query will fail. When you leave this field blank, the IVE uses the filter and base DN from the dialog to search the group objects.

## Changes to authorization groups

In IVE version 3.x, resource control is defined by the authorization group to which a user is mapped. When a user signs in, the IVE evaluates the server's group mapping rules to determine to which authorization groups the user maps. If the user maps to more than one authorization group, then the IVE presents a list of groups, from which the user must choose in order to determine which resources are available for the session. In IVE 4.0, a user is mapped to a role, which specifies access features<sup>8</sup> the user may use but does not exact complete control over which resources a user may access. IVE 4.0 enables you to grant resource accessibility based on two separate evaluation processes—first, determining who the user is, and second, by evaluating the access policy for a resource; you specify role mapping rules to determine who a user is, and you configure resource policies to determine which resources are available to that user.

When upgrading, a 3.x authorization group is migrated to 4.0 roles and resource policies. When a user signs in to a 4.0 system, the IVE displays the list of roles to which the user maps<sup>9</sup> (this list corresponds to the list of 3.x groups) and the user chooses a role for the duration of the session. This role grants the same access to resources as the 3.x authorization group. Once you migrate a 3.x system to 4.0, however, you can begin adding more detailed restrictions to specific resources and enhance the overall user experience by granting a user access to *all* appropriate resources through a permissive merge of eligible roles. A **permissive merge** is

---

<sup>8</sup> An *access feature* is an access mechanism the IVE may grant to a user, such as Web, file, application, network, meeting, and email access. 3.x offers the same access features.

<sup>9</sup> If the user maps to just one role, then the IVE does not present a list and just assigns the role's resource controls to the user.

the merging of all access options from each role to which a user maps. With respect to IVE version 3.x, this action is equivalent to granting a user access to all resources granted by each authorization group to which the user maps, but within the same user session.

This section summarizes a 3.x authorization group and describes 4.0 user roles and resource policies to provide context for how a 3.x configuration migrates to version 4.0. The function of a role and resource policy is described in more detail in the online Help (HTML format) and *Administration Guide* PDF, which is available from the online Help and on the NetScreen Support Site.

## 3.x Authorization Group Definition

In IVE version 3.x, an authorization group specifies user session properties and resource accessibility for users mapped to the group.

### A 3.x authorization group specifies:

- User accessibility to the group based on the user's IP address, browser-type, client-side certificate status, and configuration for Host Checker or Cache Cleaner. Configured here:

Authorization Group > *GroupName* > Authentication sub-tabs for all options except Cache Cleaner, which is on the Authorization Group > *GroupName* > Web tab

- Session parameters, including:

- Session settings: timeout values (idle, maximum, and reminder), timeout warning, roaming session, and single sign-on.

All on Authorization Group > *GroupName* > General > Session sub-tab except for single-sign-on, which is on Authorization Group > *GroupName* > Authentication > Remote SSO sub-tab

- Session options: Persistent password caching, persistent session cookie, and browser request follow-through options.

Authorization Group > *GroupName* > General > Options sub-tab

- Access features, which are the *types* of access mechanisms enabled for the user, including Web, file, email, application, telnet/SSH, network, and meeting. You enable/disable an access feature on these tabs:

Web browsing—Authorization Group > *GroupName* > Web > General sub-tab  
 File browsing—Authorization Group > *GroupName* > Files tab  
 Secure Email Client—Authorization Group > *GroupName* > Email Client tab  
 Secure Application Manager—Authorization Group > *GroupName* > Applications > General sub-tab  
 Secure Terminal Access—Authorization Group > *GroupName* > Applications > General sub-tab  
 Network Connect—Authorization Group > *GroupName* > General > Network Connect sub-tab  
 Secure Meeting—Authorization Group > *GroupName* > Meetings tab

For the Web and Secure Application Manager access features, there are associated options that are configured at the group level. The access features that have such options include:

Web browsing—Selective Rewrite Settings accessed on the Authorization Group > *GroupName* > Web > General sub-tab  
 Web browsing—Remote SSO Settings accessed on the Authorization Group > *GroupName* > Web > General sub-tab  
 Web browsing—Cache Cleaner Settings accessed on the Authorization Group > *GroupName* > Web > General sub-tab  
 Web browsing—Pass-through Proxy Settings accessed on the Authorization Group > *GroupName* > Web > General sub-tab  
 Secure Application Manager—with J-SAM enabled on the Authorization Group > *GroupName* > Applications > Secure Application Manager sub-tab, you can configure MS Exchange or Lotus Notes servers or Citrix nFuse settings either by clicking on their respective links on the Secure Application Manager sub-tab or by clicking on their respective sub-tabs that appear at the same level as the Secure Application Manager sub-tab after enabling J-SAM

- User resource polices, which are ACLs (Access Control Lists) that specify to which servers a client may connect. The following access features have associated ACLs:

Web browsing—Authorization Group > *GroupName* > Web > Access Control sub-tab  
 Web Java applet support—Authorization Group > *GroupName* > Web > Java Socket ACL sub-tab  
 File browsing—Authorization Group > *GroupName* > Files > Windows Access sub-tab  
 File browsing—Authorization Group > *GroupName* > Files > UNIX Access sub-tab  
 Secure Application Manager—W-SAM "Access Control" link on either the Authorization Group > *GroupName* > Applications > General sub-tab (under "Enable Secure Application Manager" or Authorization Group > *GroupName* > Applications > Secure Application Manager sub-tab,

Add Hosts page (accessed after clicking Add Hosts button)  
 Network Connect—Authorization Group > *GroupName* > General > Network Connect sub-tab

- User bookmarks, which are pre-defined bookmarks that connect the user directly to either Web or file resources or initiate an application or telnet session when clicked. The following access features may have associated bookmarks:

Web browsing—Authorization Group > *GroupName* > Web > Bookmarks sub-tab  
 File browsing—Authorization Group > *GroupName* > Files > Windows Bookmarks sub-tab  
 File browsing—Authorization Group > *GroupName* > Files > UNIX Bookmarks sub-tab  
 Secure Application Manager—W-SAM or J-SAM bookmarks can be configured on the  
 Authorization Group > *GroupName* > Applications > Secure Application Manager sub-tab  
 Secure Terminal Access—Authorization Group > *GroupName* > Applications > Terminal Sessions sub-tab

Because the 3.x authorization group controls *all* aspects of user resource accessibility, you need to create an authorization group for *each* set of specific access control settings you want to assign to a particular type of user. In IVE 4.0, you apply one level of access control to users by assigning them to one or more user roles, each of which grants them certain access features. You apply a second level of access control by defining resource policies that are evaluated only when a user makes a request to the corresponding resource. This decoupling of *who a user is* from *to whom a resource is accessible* provides you with more flexible and granular control over your resources.

## 4.0 User roles

In IVE version 4.0, a **user role** is an entity that defines user session parameters (session settings and options), personalization settings (user interface customization and bookmarks), and enabled access features (Web, file, application, network, meeting, and email access). A 4.0 IVE user role does **not** specify resource access control (ACLs) or other resource-based options<sup>10</sup> for an individual request. For example, a user role may define whether or not a user can perform Web browsing, however, the individual Web resources that a user may access are defined by Web resource policies that are configured separately in the 4.0 system.

### A 4.0 user role specifics:

- **Role restrictions**—User accessibility to the role based on source IP, user-agent, client-side certificate, Host Checker, and Cache Cleaner requirements that need to be met before a user is mapped to this role.
- **Session parameters**—Session settings, including timeout values (idle, maximum, and reminder), timeout warning, roaming session, and single sign-on, and session options, including persistent password caching, persistent session cookie, and browser request follow-through.
- **User interface options**—Personalization settings including the sign-in page, page header, page footer, and whether or not to display the browsing toolbar. In 3.x, you can customize the user interface for end-users at the system level only, meaning all users see the same user interface. In 4.0, end-users see the user interface you specify for the role to which they are mapped. If the user maps to more than one role, then the IVE displays the user interface corresponding to the first role to which a user is mapped.
- **Web settings**—Web access feature enabled or not, Web bookmarks defined for this role, and Web browsing options. The latter may include:
  - Browsing options: User can type URLs, Allow Java applets, Mask hostnames while browsing (new in 4.0), Unrewritten pages open in new window (new in 4.0)
  - Bookmark options: User can add bookmarks, Auto-allow role bookmarks (new in 4.0; selected by default when upgrading to preserve backwards compatibility).
  - Cookies options: Persistent cookies

<sup>10</sup> In 3.x, the authorization group configuration serves as the resource policy applied to user requests. An authorization group may enable a certain *type* of access feature (such as Web browsing), and this access feature may have an associated access control list (ACL) that specifies resources (servers) to which the user may or may not connect. Other access feature options may also affect how a user request is handled. Examples of “other access feature options” include the selective rewriting and pass-through proxy settings for Web browsing. In 3.x, an ACL combined with any other group settings that control the IVE’s response to a user request formulate the “resource policy” applied to the user’s request.

- **File settings**—File access feature enabled or not, file bookmarks defined for this role, and file browsing options. The latter may include:
  - Windows network files: User can browse network file shares, User can add bookmarks, and Users can add personal bookmarks to Windows folders
  - UNIX network files: User can browse network file shares, User can add bookmarks, and Users can add personal bookmarks to UNIX/NFS directories
- **Telnet/SSH settings**—Secure Terminal Access access feature enabled or not, telnet/SSH session settings bookmarked for this role, and telnet/SSH options. The latter may include:
  - User can add sessions
  - Auto-allow role Telnet/SSH sessions (new in 4.0; selected by default when upgrading to preserve backwards compatibility).
- **SAM settings**—Secure Application Manager access feature enabled or not (including whether it is J-SAM or W-SAM), W-SAM or J-SAM applications bookmarked for this role, and SAM options. The latter may include:
  - General Secure Application Manager options: Auto-launch Secure Application Manager, Auto-uninstall Secure Application Manager (new in 4.0), Auto-allow application servers (new in 4.0; selected by default when upgrading to preserve backwards compatibility).
  - Windows SAM options: Auto-upgrade Secure Application Manager (new in 4.0)
  - Java SAM Options: User can add applications, Automatic host-mapping
- **Network Connect settings**—Network Connect access feature enabled or not and the option to allow access to local subnet (new in 4.0)
- **Secure Meeting settings**—Secure Meeting access feature enabled or not and Secure Meeting options. The following may include:
  - General options: Join and create, authentication requirements, password distribution, remote control
  - Policy settings for number of scheduled meetings, simultaneous meetings, simultaneous meeting attendees, duration of meetings

When comparing a 4.0 user role to a 3.x authentication group, you can see that the options you configure for a 3.x authorization group map directly to the options you may specify for a 4.0 user role (excluding user interface options, as noted above).

## 4.0 Resource policies

In IVE version 4.0, a **resource policy** is a policy that specifies resources or actions for a particular access feature. A **resource** is either a server or file that can be accessed through the IVE, and an **action** is to “allow” or “deny” a resource or to perform or not perform a function. Each access feature has one or more types of policies, which determine the IVE’s response to a user request.

### A 4.0 resource policy may be one of the following types:

- **Web Resource Policies**—The Web access feature has the following types of resource policies:
  - Access: Specifies Web resources to which users may or may not browse
  - Caching: Specifies for which Web resources the IVE sends or modifies page headers
  - Java Access: Specifies to which servers Java applets may connect
  - Java Signing: Specifies whether to re-sign Java applets with an applet certificate or the default IVE certificate
  - Selective Rewriting: Specifies resources for the IVE to re-write or not
  - Pass-through Proxy: Specifies Web applications for which the IVE performs minimal intermediation
  - Form POST: Specifies whether or not to post a user’s IVE credentials directly to a back-end Web application’s sign-in form

- Cookies/Headers: Specifies whether or not to post cookies and headers to a back-end Web application's sign-in form
- **File Resource Policies**—The File access feature has the following types of resource policies:
  - Windows Access: Specifies Windows file resources to which users may or may not browse
  - Windows Credentials: Specifies credentials for the IVE to submit to a file server
  - UNIX/NFS Access: Specifies UNIX/NFS file resources to which users may or may not browse
- **Secure Application Manager Resource Policies**—The Secure Application Manager access feature has one type of resource policy: Allow or deny applications configured to use J-SAM or W-SAM to connect to application servers
- **Telnet/SSH Resource Policies**—The Telnet/SSH access feature has one type of resource policy: Allow or deny access to the specified servers
- **Network Connect Resource Policies**—The Network Connect access feature two types of resource policies:
  - Access: Specifies to which resources users may connect using Network Connect
  - IP Address Pools: Specifies an IP pool from which the IVE assigns an IP address to both the server- and client-side processes for a Network Connect session
- **Secure Meeting Resource Policies**—The Secure Meeting access feature has one type of resource policy: Enable or disable email notifications to people invited to a secure meeting
- **Secure Email Client Resource Policies**—The Secure Email Client access feature has one type of resource policy: Enable or disable email client support

When comparing a 4.0 resource policy to a 3.x authentication group, you can see that the resources you configure for a 3.x authorization group map directly to the resources you specify in a 4.0 resource policy.

### 3.x Authorization Group Migration Path

In 3.x, you configure resource accessibility for a group of users in one place—on the Authentication & Authorization > Authorization Groups > *GroupName* page. In 4.0, you configure resource accessibility in two places:

- You specify user roles, to which authenticated users are mapped if they meet the role mapping requirements, on the Users > Roles page.
- You specify resource policies that the IVE evaluates when receiving a user request on the Resource Policies pages—Web, Files, SAM, Telnet/SSH, Network Connect, Meetings, and Email Client.

When you upgrade a 3.x configuration to 4.0, the upgrade process creates the following entities for *each* authorization group:

- **A 4.0 user role**

The IVE uses the 3.x authorization group name to name the role. For example, if the 3.x authorization group name is "marketing," then the IVE creates a 4.0 user role on the Users > Roles page called "marketing." The user role definition specifies which access features are enabled for the role, as well as bookmarks (Web, file, application, and telnet/SSH session) and related options. For information about where specific 3.x options migrate, refer to "Reference B: User Interface Mapping—3.x to 4.0" on page 27.

- **4.0 resource policies**

The IVE creates a 4.0 a resource policy for each 3.x access control list (ACL). A 3.x ACL is a list of resources to which you either allow or deny access. An ACL works in conjunction with an "open" or "closed" policy. In 3.x, an *open policy* grants access to all resources (related to the access feature) except for those specified in the ACL; a *closed policy* denies access to all resources (related to the access feature) except for those specified in the ACL.

For example, if you enable the Web access feature, the default 3.x policy is “open,” meaning that users may access any Web servers. If you add servers to the ACL, then users can access all servers except for those in the list. The opposite is true for a closed policy—users may not access any Web servers except for those in the ACL. You can configure ACLs for both an open and closed policy, and the IVE stores this information so that you can toggle between the two without having to re-create the corresponding ACL when you switch back and forth.

When you upgrade from 3.x to 4.0, however, the upgrade process creates one resource policy corresponding to the access feature’s *active* policy. Specifically, if the open policy is active, then the upgrade process creates a resource policy that allows access to all servers except for any defined in the 3.x ACL, which migrate to a separate “Deny” resource policy (created first, if applicable). The converse is true for a closed policy. Because data from only the active policy migrates, you may want to create additional resource policies after upgrading that address the same conditions as the 3.x inactive policies that do not migrate.

## Specific Resource Policy Details

This section describes how specific 4.0 resource policies are created from a 3.x authorization group configuration. Note that a policy applies only to the role corresponding to the 3.x authorization group from which it is created. For information about how 3.x system-level settings migrate, see “Miscellaneous Upgrade Details

” on page 21.

### Web Resource Policies

#### Access

- If the 3.x group has an open policy, then the upgrade process creates a 4.0 Web Access policy with the action “Allow” and the resources specified as “\*:\*” (all). To represent the 3.x ACL corresponding to the open policy, the upgrade process creates a 4.0 Web Access policy with the action “Deny” and lists each resource from the ACL. This policy is ordered before the “Allow” policy.
- If the 3.x group has an open policy and its ACL denies resources by IP address (vs. hostname), then the upgrade process creates a 4.0 Web Access policy with the action “Allow” and the resources specified as “\*[a-zA-Z]\*:\*” (meaning that the hostname of the requested resource must contain at least one alpha character (in effect, not be an IP address) in order for the IVE to serve the request).
- If the 3.x group has a closed policy, then the upgrade process creates a 4.0 Web Access policy with the action “Allow” and the resources specified as all of the resources from the 3.x Web ACL.

Note: Regardless of whether or not a 3.x group uses an open or closed policy for Web access, the “Auto-allow role bookmarks” checkbox on the Roles > *RoleName* > Web > Options tab of the role corresponding to the 3.x authorization group is checked after the upgrade. This option tells the IVE to automatically create a Web Access resource policy that allows user access to the resource specified by a Web bookmark created on a Roles > *RoleName* > Web > Bookmarks tab. This action ensures that users will be able to access a bookmarked resource. Note that this behavior applies only to role bookmarks, not user bookmarks.

#### Java

- If the 3.x group enables Java applet support with full network connectivity (3.x Web > General tab), then the upgrade process creates a 4.0 Web Java Access policy with the action “Allow” and the resources specified as “\*:\*” (all).
- If the 3.x group enables Java applet support with access control, then the upgrade process creates a 4.0 Web Java Access policy with the action “Allow” and the resources specified as all of the resources from the 3.x Java Socket ACL.
- If your 3.x configuration specifies applet certificates to use with trusted servers (3.x System > Certificates > Applet Certificates tab), then the upgrade process creates a 4.0 Java Code Signing policy with no action specified but with the resources specified as all of the resources from the Trusted Servers list on the 3.x

Applet Certificates tab. Note that when upgrading, the 3.x “Trusted Servers” list on the System > Certificates > Applet Certificates tab migrates to a Java Code Signing policy (on the 4.0 Resource Policies > Web > Java > Code Signing tab) that applies to every role created from the 3.x configuration. See the “Miscellaneous Upgrade Details

- “ section on page 21 for information about upgrading vs. importing 3.x configuration files to 4.0.)

### Rewriting

- If the 3.x group disables Selective Rewriting, then the upgrade process creates a 4.0 Selective Rewriting policy with the action “Rewrite” and the resources specified as “\*:\*” (all).
- If the 3.x group enables Selective Rewriting, then the upgrade process creates three 4.0 Selective Rewriting policies in this order:
  1. A “Don’t Rewrite” policy that specifies the resources (URLs) specified on the 3.x Authentication & Authorization > Authorization Groups > *GroupName* > Web > General > “Selective Rewrite Settings” link > Selective Rewrite Settings page in the “Exception URLs” list.
  2. A “Rewrite” policy that specifies the resources (URLs) specified on the 3.x Authentication & Authorization > Authorization Groups > *GroupName* > Web > General > “Selective Rewrite Settings” link > Selective Rewrite Settings page in the “Rewrite” list.
  3. A “Don’t Rewrite” policy that specifies the resources as “\*:\*” (all).

### Remote SSO

4.0 Remote SSO resource policies are based on 3.x Remote SSO Bookmarks. Policies are created as follows:

- If your 3.x configuration does not have any Remote SSO bookmarks, then no 4.0 policies are created, even if Remote SSO is enabled for the group.
- A 3.x Forms-based SSO bookmark migrates to a 4.0 Form Post policy. If the 3.x group “Allow direct login to backend application” is disabled, then the upgrade process checks the “Deny direct login for this resource” check box for each Form POST policy.
- A 3.x Custom Headers and Cookies bookmark migrates to a 4.0 Headers/Cookies policy.

Note that there is no corresponding “Allow Single Sign On only from bookmarks page” functionality in 4.0 since there is no Single Sign On bookmark in 4.0.

### File Resource Policies

#### Windows

If the 3.x group Windows Access policy is **open**:

- The upgrade process migrates the 3.x Windows bookmarks to 4.0 Windows bookmarks—3.x Authentication & Authorization > Authorization Groups > *GroupName* > Files > Windows Bookmarks tab to 4.0 Users > Roles > *RoleName* > Files > Windows Bookmarks tab—and unchecks the “Enable auto-allow access to this bookmark” checkbox on each bookmark’s configuration page. These bookmarks appear on a user’s Bookmarks page under “Folder Bookmarks.”
- The upgrade process creates a “Deny” Windows Access policy that lists the resources from the 3.x open policy’s ACL (Deny Windows Resource); these resources are the denied file servers specified for the 3.x open policy’s ACL. The upgrade process also creates an “Allow” policy that specifies “\*:\*” as the resource. This policy denies user requests to the first set of resources and allows access to all other file servers.
- If the 3.x group Windows Access setting enables users to browse resources, then the upgrade process checks the “User can browse network file shares” checkbox on the 4.0 Users > Roles > *RoleName* > Files > Options tab.

If the 3.x group Windows Access policy is **closed**:

- The upgrade process migrates the 3.x Windows bookmarks for the group to 4.0 Windows bookmarks—3.x Authentication & Authorization > Authorization Groups > *GroupName* > Files > Windows Bookmarks tab to

4.0 Users > Roles > *RoleName* > Files > Windows Bookmarks tab—and unchecks the “Enable auto-allow access to this bookmark” checkbox on each bookmark’s configuration page. These bookmarks appear on a user’s Bookmarks page under “Folder Bookmarks.”

- For the 3.x closed policy’s ACL (Allow Windows Resource), the upgrade process creates on access-point<sup>11</sup> bookmark:
    - If the 3.x ACL has file extension filtering turned off—the 3.x “Show only files of a specific type” checkbox is not checked—the upgrade process creates a 4.0 access-point bookmark with “Enable auto-allow access to this bookmark” turned on to appropriately support the 3.x “Read only” and “Show subdirectories (if any)” settings.
    - If the 3.x ACL has file extension filtering turned on—the 3.x “Show only files of a specific type” checkbox is checked—the upgrade process creates a 4.0 access-point bookmark with “Enable auto-allow access to this bookmark” turned off but the corresponding Windows Access resource policy that maps to the role has a detailed rule written as follows:
      - If the 3.x ACL is set to show subfolders, then the 4.0 resource policy’s detailed is set as: “Allow,” the resource is \\server\share\path\\*.filter (where filter is the file extension) and the “Read-only” option is selected, if appropriate
      - If the 3.x ACL is set not to show subfolders, then the 4.0 resource policy’s detailed is set as: “Allow,” the resource is \\server\share\path\%o.filter (where filter is the file extension) and the “Read-only” option is selected, if appropriate
- Note:
- \* Matches any character
  - % Matches any character except backslash (\), which means subfolders are not matched and users cannot access them
- The upgrade process checks the “User can browse network file shares” checkbox on the role’s Users > Roles > *RoleName* > Files > Options tab if any of the options on the 3.x Authentication & Authorization > Authorization Groups > *GroupName* > General tab enable users to view *any* allowed resources.

## UNIX/NFS

3.x UNIX/NFS file configuration only has a closed policy, which the upgrade process migrates the same as it migrates the closed policy for Windows files.

## Telnet/SSH Resource Policies

- If a 3.x group enables Secure Terminal Access with the “User can add bookmarks” option, then the upgrade process checks the “User can add sessions” checkbox on the 4.0 Users > Roles > *RoleName* > Telnet/SSH > Options tab and creates an “Allow” Telnet/SSH policy with “\*:\*” specified as the resource.
- If a 3.x group enables Secure Terminal Access, then for every 3.x Terminal Session bookmark, the upgrade process creates:
  - An “Allow” Telnet/SSH policy that specifies the remote host as the resource
  - A Telnet/SSH session bookmark on the 4.0 Users > Roles > *RoleName* > Telnet/SSH > Sessions tab
- For each 3.x group that enables Secure Terminal Access, the upgrade process checks the “Auto-allow role Telnet/SSH sessions” checkbox on the corresponding 4.0 role’s Users > Roles > *RoleName* > Telnet/SSH > Options tab.

## Secure Application Manager Resource Policies

### J-SAM

- Enabled MS Exchange, Lotus Notes, and Citrix NFuse servers for a 3.x group migrate to a SAM application bookmark for the corresponding role (Users > Roles > *RoleName* > SAM > Applications tab).

<sup>11</sup> An **access-point bookmark** is a bookmark to a file resource that shows up only when a user browses the available file server; it does not appear on the user’s Bookmarks page under “Folder Bookmarks.”

- For every 3.x application server configured for J-SAM, the upgrade process creates an “Allow” SAM Access policy:
  - For 3.x MS Exchange servers:
    - If the MS Exchange option is enabled *with* access control and host mapping is enabled, then the SAM Access policy specifies each 3.x Exchange server as a resource in the format:
 

```
exchange1:*
exchange2:*
...
```
  - For 3.x Lotus Notes servers:
    - If the Lotus Notes option is enabled *with* access control, then the upgrade process creates on SAM Access policy that specifies each 3.x Lotus Notes server as a resource in the format:
 

```
server:1352
server:1352
...
```
    - If the Lotus Notes option is enabled *without* access control, then the upgrade process creates one SAM Access policy that specifies the resources as “\*:1352”
- For the 3.x Citrix NFuse option, the upgrade process creates one SAM Access “Allow” policy that specifies the ports in the “List of ports” field. For example, if the 3.x configuration specifies port 1494, then the upgrade process specifies the SAM Access policy resource as: “\*:1494”
- If the 3.x J-SAM option specifies that users can add applications, the upgrade process creates an “Allow” SAM Access policy with the resource “\*:\*” and the policy applies to the roles corresponding to the 3.x groups for which this option was configured.
- For all roles corresponding to 3.x groups that enabled J-SAM, the “Auto-allow application servers” option is checked.

### W-SAM

- The W-SAM option (with or without NetBIOS) enabled for a 3.x group migrates to a SAM application bookmark for the corresponding role.
- The upgrade process creates one “Allow” SAM Access policy for each 3.x group that specifies a W-SAM ACL (access control list). Each server in the ACL is listed as a resource.

### Network Connect

- The upgrade process creates one Access policy that specifies each IP address from the Access Control list on the 3.x Authentication & Authorization > Authorization Groups > *GroupName* > General > Network Connect tab.
- The upgrade process creates one IP Address Pools policy that specifies each IP address and IP range from the Client Address Pool list on the 3.x Authentication & Authorization > Authorization Groups > *GroupName* > General > Network Connect tab.

Note that the upgrade process checks the “Allow access to local subnet” checkbox for a role (Users > Roles > RoleName > Network Connect tab) unless the 3.x group enables Network Connect without split-tunneling.

### Miscellaneous Upgrade Details

There are two ways to migrate your IVE 3.x system to IVE 4.0:

- Install a 4.0 service package on your 3.x IVE appliance.
- Import 3.x system, user, ACL, and bookmark configuration files into a 4.0 IVE appliance.

When you install a 4.0 service package, the following settings are carried over to the 4.0 configuration:

- 3.x Web proxy settings, which are specified at the system level on the 3.x Network > Web Proxy page, are copied to the 4.0 Resource Policies > Web > Web Proxy > Settings tab, and the upgrade process creates a corresponding Web Proxy resource policy that applies to every role created from the 3.x configuration.
- 3.x content caching settings, which are specified at the system level on the 3.x System > Settings > Security > Content Caching tab, are copied to a Web Caching resource policy that applies to every role created from the 3.x configuration.
- The 3.x "Trusted Servers" list on the System > Certificates > Applet Certificates tab migrates to a Java Code Signing policy (on the 4.0 Resource Policies > Web > Java > Code Signing tab) that applies to every role created from the 3.x configuration.

If you import 3.x configuration files to a 4.0 system, these three pieces of data are lost.

Other details about the upgrade process:

- When configuring an authorization group in 3.x, you can specify to use either the "Users group" settings or "custom settings" for every aspect of group configuration. During the upgrade process, the IVE uses the Users group configuration information when required to create the corresponding 4.0 configuration. Note that in IVE 4.0, a role does not inherit settings from another role.
- The 3.x Administrators group migrates to a 4.0 ".Administrators" and a ".Read-Only Administrators" role. These two roles appear on the 4.0 Administrators > Delegation page. The settings and options in these roles are based on the 3.x Administrators group settings and options and are identical to each other.
- In IVE 4.0, you can configure "default options" for administrator and user roles. These default options are based on the settings for the Administrators group and Users group, respectively.
- If a 3.x authorization group access feature is configured to inherit an ACL from the Users group, the IVE does not create the corresponding resource policy when upgrading that particular group. Instead, when the 3.x Users group migrates to 4.0, all of its ACLs are converted to 4.0 resource policies, and then the new 4.0 resource policy (previously a 3.x ACL that was inherited by a 3.x group) applies to the appropriate 4.0 role(s). Note that in IVE 4.0, resource policies are closed, meaning that users have no access to Web, file, application, network, meeting, and email resources until you specifically grant access through a resource policy.
- The 4.0 General > Overview tab for an administrator or user role has a Session Options check box that is selected after the upgrade process if the 3.x authorization group had custom values for its session properties.
- In 3.x, the frequency update for Cache Cleaner is specified per group. In 4.0, these values are global (specified on the System > Configuration > Security > Cache Cleaner tab). During migration, the upgrade process copies the frequency values from the first 3.x group that specifies them.

Also, if a 3.x authorization group had Cache Cleaner enabled, then:

- The 4.0 authentication realm created from the 3.x server to which the authorization group maps requires that the IVE load Cache Cleaner on the user's machine. This requirement is specified in the realm's authentication policy and applies to any user who chooses the realm when signing in.
- The 4.0 role created from the 3.x authorization group is set to enable Cache Cleaner (on the 4.0 Users > Roles > *RoleName* > General > Restrictions > Cache Cleaner tab).
- In 3.x, Host Checker policies are specified per group. In 4.0, Host Checker policies are global (specified in System > Configuration > Security > Host Checker tab). The upgrade process copies all the 3.x Host Checker policies defined in 3.x authorization groups, even if the Host Checker option is disabled for the group (on the 3.x Authentication & Authorization > Authorization Groups > *GroupName* > Authentication > Host Checker tab). All copied Host Checker policies are listed on the 4.0 System > Configuration > Security > Host

Checker tab. Also, if a 3.x authorization group had Host Checker enabled, then:

- The 4.0 authentication realm created from the 3.x server to which the authorization group maps requires that Host Checker is loaded on the user's machine. This requirement is specified in the realm's authentication policy and applies to any user who chooses the realm when signing in.

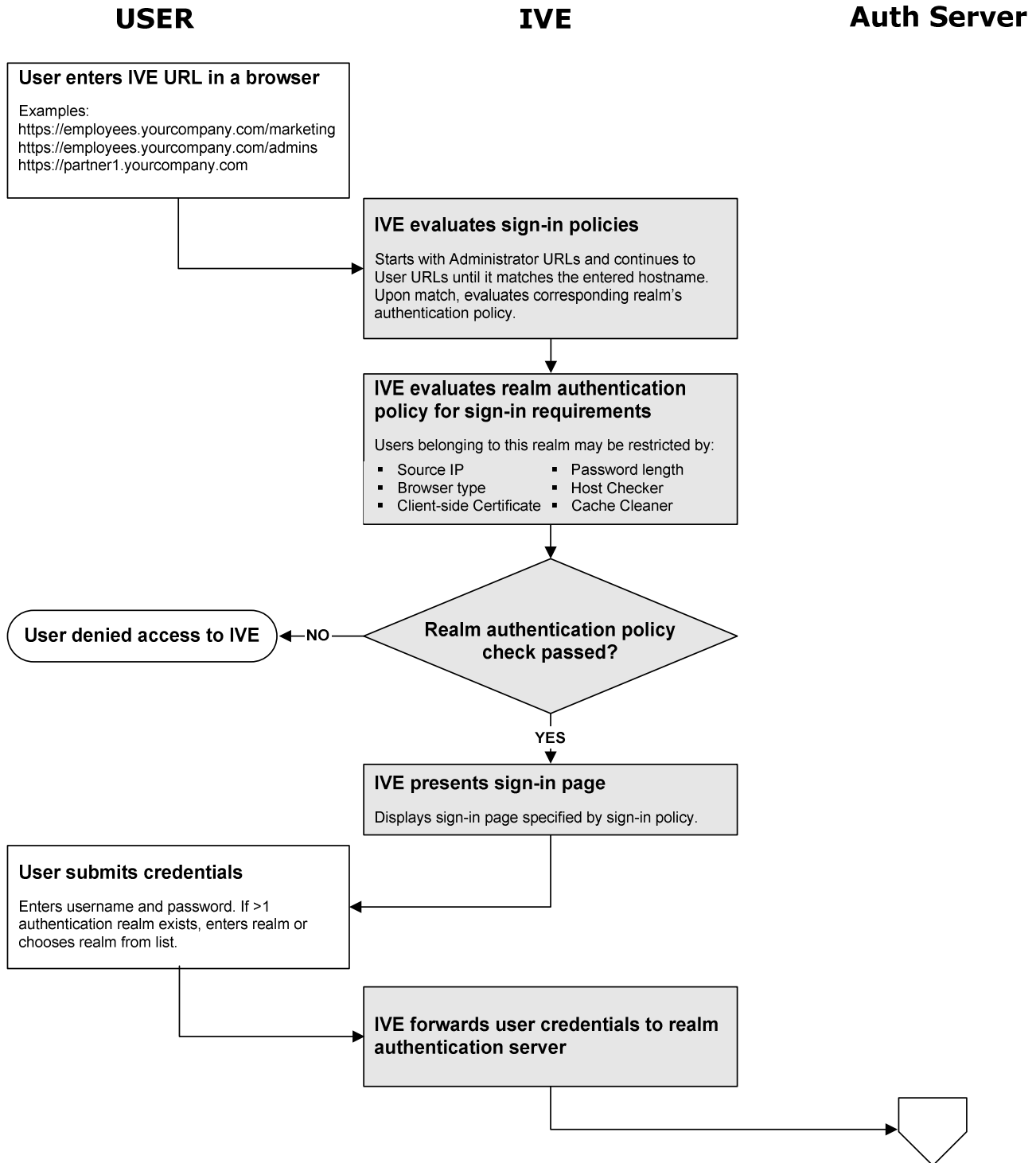
- The 4.0 role created from the 3.x authorization group is set to enable Host Checker (on the 4.0 Users > Roles > *RoleName* > General > Restrictions > Host Checker tab). The Host Checker policies specified for the 3.x group are listed as required policies for the role.
- If a 3.x group requires a client-side certificate, then the upgrade process specifies this requirement in the authentication policy for the realm that corresponds to the 3.x server to which the 3.x authorization group was mapped.
- The resource policies for Secure Meeting and Secure Email Client are system-wide settings; any role for which you enable these access features uses the settings specified by the feature’s respective resource policy (Secure Meeting or Secure Email).

## Upgrade Summary

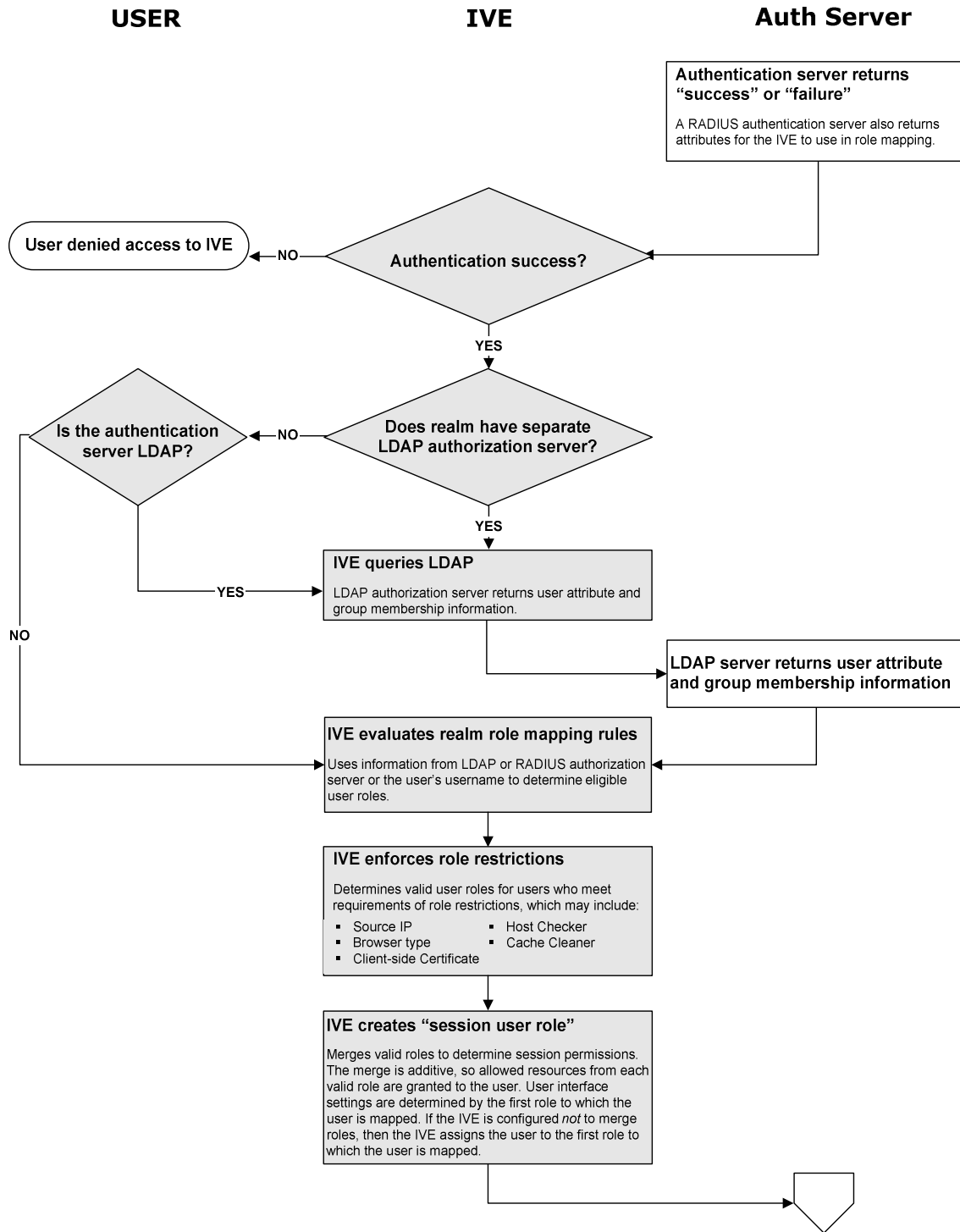
| IVE version 3.x  | IVE version 4.0  |
|--|--|
| A 3.x authentication server is defined in this menu: Authentication & Authorization > Authentication Servers   | A 4.0 authentication server is defined in this menu: System > Signing In > Servers   |
| A 3.x authentication server is a stand-alone entity for verifying a user’s credentials and granting access to the IVE.   | A 4.0 authentication server is part of a larger entity—an authentication realm—and while still used to verify a user’s credentials, it is not the sole mechanism for granting access to the IVE; a user must also comply with the realm’s authentication policy.   |
| A 3.x authentication server receives a user’s credentials from the IVE when a user signs in.   | A 4.0 authentication server receives a user’s credentials from the IVE only if the user conforms to the authentication policy defined for the realm.   |
| A 3.x authentication server verifies a user’s credentials and then the IVE uses the group mapping rules defined as part of the authentication server’s configuration to determine to which IVE group to assign a user. | A 4.0 authentication server verifies a user’s credentials and then the IVE uses the role mapping rules defined for the authentication realm to determine to which roles a user is eligible to be mapped.   |
| A 3.x authorization group determines which access features, server resources (Web, file, application), session options, and bookmarks (Web, file, application) are available for a user’s session.                     | A 4.0 user role determines which access features are available (Web, file, SAM, Telnet/SSH, Network Connect, Meetings, Email Client) for a session, as well as session-related options for those features and corresponding bookmarks.<br>A 4.0 resource policy determines server resources (Web, file, and application) that a user may access. |
| A user must choose a 3.x authorization group (if the authenticated user maps to more than one group) and the group’s configuration applies to the session.   | A user may choose a 4.0 role (if the authenticated user maps to more than one role) and the role’s configuration applies to the session or you can configure the IVE to merge the permissions from all roles to which the user maps.   |
| The IVE determines to which authorization groups a user maps based on group mapping rules defined for the authentication server (chosen when the user signs in).   | The IVE determines to which user roles a user maps based on both the role mapping rules defined for the authentication realm (chosen when the user signs in) and any restrictions defined for each role.   |
| Data retrieved from an authorization server to use when determining group membership (by a group mapping rule) may not be used in further evaluations.   | Data retrieved from an authorization server to use when determining role eligibility (by a role mapping rule) may be used by resource policies to determine user resource access.  |
| The 3.x Users group is the only mechanism for defining baseline settings that other groups may inherit.  | The 4.0 Access Management system decouples role-based settings from specific file and application server access control, enabling resource policies to apply to more than one role.  |

## Reference A: Authentication and Authorization Flowchart

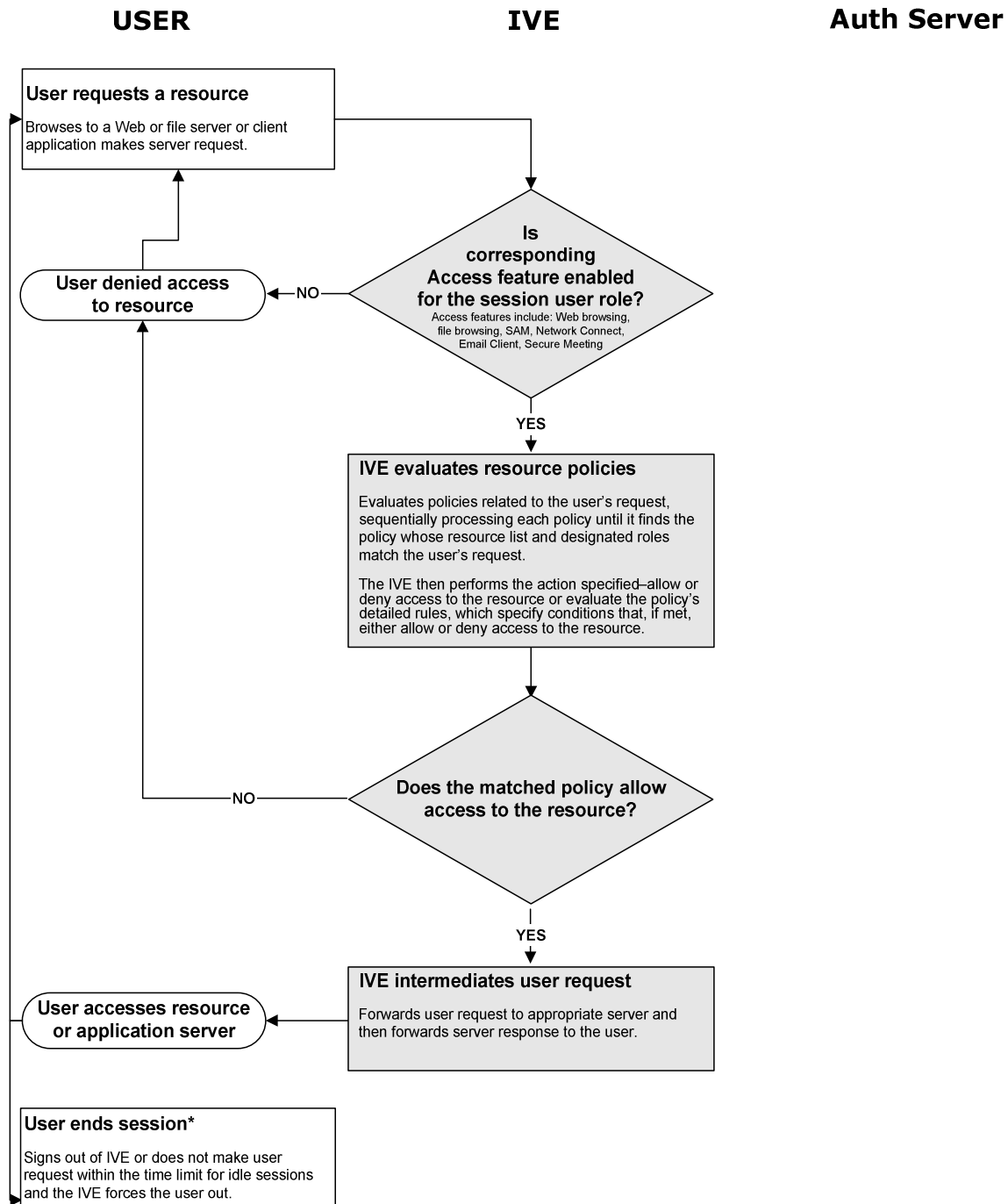
This flowchart shows the transactions that take place between a user and the IVE and the IVE and an authentication realm. The flowchart begins with a user entering the URL to an IVE sign-in page and ends with the user proactively ending the user session.



### Step 1 of 3: IVE authenticates user



**Step 2 of 3: IVE maps user to one or more user roles**



\*At any point during a user session, the IVE may force the user out if the user session reaches the maximum session length.

**Step 3 of 3: IVE evaluates resource policies corresponding to user request**

## Reference B: User Interface Mapping—3.x to 4.0

The table below maps user interface elements in version 3.x of the IVE to where they are in version 4.0. User interface elements include menus, tabs, sub-tabs, and specific settings on a page. Please use this guide to become familiar with the 4.0 Administrator Console and notify your account manager if you find discrepancies between what's listed in the table and what you find on the user interface. Also, note that this table does not provide conceptual mapping. To help you understand the changes you'll see in the UI, keep these details in mind:

- 3.x Authorization Groups → 4.0 User Roles**

A 3.x authorization group is converted to a "user role" in 4.0. In 4.0, a user is mapped to a user role instead of an IVE group. Also in 4.0, there's no concept of an "IVE group." Groups in 4.0 now refer only to LDAP or RADIUS groups.

- 3.x Authentication Servers → 4.0 Servers**

A 3.x authentication server is defined through the top-level menu "Authentication & Authorization > Authentication Servers." In 4.0, authentication servers are moved to a sub-tab of a System menu: "System > Signing In > Servers." In 3.x, users select an authentication server when signing in, and the group mapping rules defined for the server determine the user's permissions (as defined by authorization group to which the user is mapped). In 4.0, users select an authentication realm when signing in, which specifies one authentication server, one authorization server (optional), one authentication policy, and role mapping rules. If the user is authenticated, then the IVE evaluates the realm's role mapping rules to determine to which user roles to map a user.

- 3.x Group Mapping Rules → 4.0 Role Mapping Rules**

3.x group mapping rules are part of the authentication server definition. In 4.0, users are mapped to roles (instead of groups) by role mapping rules. Role mapping rules are defined as part of a realm definition: Administrators (or Users menu) > Authentication > New > Role Mapping.

| 3.x User Interface Element       | 4.0 User Interface Element   |
|----------------------------------|--|
| <b>System menus</b>              |  |
| <b>System &gt; Settings menu</b> |  |
| General tab                      |  |
| Logging Disk                     | System > Status > Overview   |
| Number of Sign-In Users          | System > Status > Overview   |
| System Software Pkg Version      | System > Status > Overview   |
| Allowed SSL Version              | System > Configuration > Security > Security Options               |
| Allowed Encryption Strength      | System > Configuration > Security > Security Options               |
| Page Caching                     | Resource Policies > Web > Caching > Policies > <i>SelectPolicy</i> |
| Browsing to SSL Sites            | System > Configuration > Security > Security Options               |
| Time Since Last Reboot           | System > Status > Overview   |
| Reboot Now                       | Maintenance > System > Platform                                    |
| Shutdown                         | Maintenance > System > Platform                                    |
| Servers Connectivity             | Maintenance > System > Platform                                    |
| License tab                      | System > Configuration > Licensing                                 |
| Security > General sub-tab       |  |
| Allowed SSL and TLS Version      | System > Configuration > Security > Security Options               |

### 3.x User Interface Element

### 4.0 User Interface Element

Allowed Encryption Strength

System > Configuration > Security > Security Options

Browsing to SSL Sites

System > Configuration > Security > Security Options

Basic Authentication Intermediation

System > Configuration > Security > Security Options (not in Beta)

Sign-In Password Length

Administrators > Authentication > *SelectRealm* > Authentication Policy > Password AND Users > Authentication > *SelectRealm* > Authentication Policy > Password

Automatic Version Monitoring

Maintenance > System > Options (*not in Beta*)

Neoteris Communication Protocol for Client-Server Applications

System > Configuration > Security > Security Options

ZIP Accelerator

Maintenance > System > Options (*not in Beta*)

SSL Accelerator

Maintenance > System > Options (*not in Beta*)

Security > Content Caching sub-tab

All options except Max File Size

Resource Policies > Web > Caching > Policies > *SelectPolicy* > General

Max File Size option

Resource Policies > Web > Caching > Policies > *SelectPolicy* > Options

Time tab

System > Status > Edit > Date and Time

Log > View sub-tab

System > Log/Monitoring > Events > Log

Log > Settings sub-tab

System > Log/Monitoring > Events > Settings

Statistics tab

System > Log/Monitoring > Statistics

Archiving tab

Maintenance > Archiving > FTP Server

Debugging > Trace sub-tab

Maintenance > Troubleshooting > Session Recording

Debugging > State sub-tab

Maintenance > Troubleshooting > System Snapshot

Debugging > TCP Dump sub-tab

Maintenance > Troubleshooting > TCP Dump

Debugging > Commands sub-tab

Maintenance > Troubleshooting > Commands

Debugging > Remote Debugging sub-tab

Maintenance > Troubleshooting > Remote Debugging

Sign-in Options > Restrictions sub-tab

System > Signing In > Sign In Policies

Sign-in Options > Authorization Mode sub-tab

Administrators > Authentication > *SelectRealm* > Role Mapping AND Users > Authentication > *SelectRealm* > Role Mapping

Encoding tab

Resource Policies > Files > Encoding

| 3.x User Interface Element                      | 4.0 User Interface Element  |
|---|---|
| <b>System &gt; Appearance menu</b>              |   |
| General tab                                     |   |
| Header (logo image & background color)          | System > Signing In > Sign In Pages > <i>SelectPage</i> > Sign-In Page AND Users > Roles > <i>SelectRole</i> > General > UI Options   |
| Browsing toolbar (show toolbar & logo image)    | Users > Roles > <i>SelectRole</i> > General > UI Options  |
| Personalize welcome message on bookmarks page   | System > Signing In > Sign In Pages > New Sign-In Page  |
| Show "Powered by Neoteris" label                | Users > Roles > <i>SelectRole</i> > General > UI Options  |
| Restore Factory Defaults                        | <i>Not directly implemented in 4.0. To restore the default system sign-in page, create a new one through the <b>System &gt; Signing In &gt; Sign-in Page</b> tab—the defaults will appear. No option is available, however, for restoring default role-based sign-in options.</i> |
|   |   |
| Sign-in Page tab                                | System > Signing In > Sign In Pages > <i>SelectPage</i> > Sign-In Page  |
| <b>System &gt; Certificates menu</b>            |   |
| Server Certificate tab                          | System > Configuration > Certificates > Server Certificates   |
| CA Certificate tab                              | System > Configuration > Certificates > CA Certificates   |
| Applet Certificate tab                          |   |
| Import Certificates                             | System > Configuration > Certificates > Applet Certificates   |
| Delete Certificates                             | System > Configuration > Certificates > Applet Certificates   |
| Trusted Server                                  | Resource Policies > Web > Java > Code Signing > <i>SelectPolicy</i>   |
|   |   |
| <b>System &gt; Import/Export menu</b>           |   |
| Configuration tab                               | Maintenance > Import/Export > Configuration   |
| User Accounts tab                               | Maintenance > Import/Export > User Accounts   |
| ACLs & Bookmarks tab                            | Maintenance > Import/Export > ACLs & Bookmarks  |
| <b>System &gt; Install Service Package menu</b> |   |
| <b>System &gt; Secure Meetings menu</b>         |   |
| General tab                                     | Resource Policies > Meetings  |
| Schedule tab                                    | System > Status > Meeting Schedule  |

### 3.x User Interface Element

### 4.0 User Interface Element

#### Authentication & Authorization menus

##### Authentication & Authorization > Administrators menu

Members tab > *SelectAdmin*

Administrators > Authentication > *SelectRealm* > General

Session tab

Administrators > Delegation > *SelectRole* > General > Session Options

Authentication > Authentication Server sub-tab

Administrators > Authentication > *SelectRealm* > General

Authentication > Address Restrictions sub-tab

Administrators > Authentication > *SelectRealm* > Authentication Policy > Source IP

Authentication > Certificate sub-tab

Administrators > Authentication > *SelectRealm* > Authentication Policy > Certificate

##### Authentication & Authorization > Authentication Servers menu

Create and Delete options

System > Signing In > Servers

Enable and Disable options

System > Signing In > Sign-in Policies

##### Authentication & Authorization > Authorization Groups menu

General > Overview sub-tab

Session

Users > Roles > *SelectRole* > General > Session Options

Features

Users > Roles > Roles

Access Control

Resource Policies > Web > Access

Bookmarks:

Web

Users > Roles > *SelectRole* > Web > Bookmarks

Windows

Users > Roles > *SelectRole* > Files > Windows Bookmarks

UNIX/NFS

Users > Roles > *SelectRole* > Files > UNIX Bookmarks

Terminal Access

Users > Roles > *SelectRole* > Telnet/SSH > Sessions

General > Network Connect sub-tab

Enable Network Connect

Users > Roles > *SelectRole* > General > Overview

Client Address Pool

Resource Policies > Network Connect > IP Address Pools

Access Control

Resource Policies > Network Connect > Access

General > Session sub-tab

Users > Roles > *SelectRole* > General > Session Options

General > Options sub-tab

Users > Roles > *SelectRole* > General > Session Options

Authentication > Authentication Server sub-tab

Administrators > Authentication AND Users > Authentication

Authentication > Address Restrictions sub-tab

Users > Roles > *SelectRole* > General > Restrictions > Source IP

Authentication > Browser Restrictions sub-tab

Users > Roles > *SelectRole* > General > Restrictions > Browser

| 3.x User Interface Element | 4.0 User Interface Element |
|----------------------------|----------------------------|
|----------------------------|----------------------------|

Authentication > Certificate sub-tab

Users > Roles > *SelectRole* > General > Restrictions > Certificate

Authentication > Remote SSO sub-tab

Resource Policies > Web > Remote SSO

Authentication > Host Checker sub-tab

|                      |
|----------------------|
| Enable/Disable       |
| Host Checking Method |
| Rule Setting         |
| Check Interval       |
| Failure Page URL     |

|  |
|--|
| Administrators > Authentication > <i>SelectRealm</i> > Authentication Policy > Host-checker AND Users > Authentication > <i>SelectRealm</i> > Authentication Policy > Host-checker AND Users > Roles > <i>SelectRole</i> > General > Restrictions > Host-checker AND Resource Policies > Web > <i>SelectPolicy</i>   |
| System > Configuration > Security > Host Checker > <i>SelectPolicy</i>   |
| System > Configuration > Security > Host Checker > <i>SelectPolicy</i>   |
| System > Configuration > Security > Host Checker   |
| <i>Not required in 4.0. In 3.x, if a user was a member of a group that required Host Checker but Host Checker was not installed on his system, he could not sign in to the IVE and needed to be directed to a failure page. In 4.0, a user may have multiple roles—some that require Host Checker and some that don't. If he does not have Host Checker on his system, he will only get the rights granted to those roles that don't require Host Checker. If the admin requires Host Checker at the realm level in 4.0 and the user doesn't have it, he will not be able to sign in to the IVE.</i> |

Web > General sub-tab

|                            |
|----------------------------|
| Enable Web Browsing        |
| Enable Java Applet Support |
| Enable Persistent Cookies  |
| Enable Selective Rewriting |
| Enabled Encoded Hostname   |
| Enable Remote SSO          |
| Enable Cache Cleaner       |
| Enable Pass-Through Proxy  |

|   |
|---|
| Users > Roles > <i>SelectRole</i> > General > Overview                          |
| Users > Roles > <i>SelectRole</i> > Web Options                                 |
| Users > Roles > <i>SelectRole</i> > Web Options                                 |
| Users > Roles > <i>SelectRole</i> > Web Options                                 |
| Users > Roles > <i>SelectRole</i> > Web Options                                 |
| Resource Policies > Web > Remote SSO  |
| Users > Roles > <i>SelectRole</i> > General > Restrictions > Cache Cleaner      |
| Resource Policies > Web > Rewriting > Pass-through Proxy ( <i>not in beta</i> ) |

Web > Access Control sub-tab

Resource Policies > Web > Access

Web > Bookmarks sub-tab

|                      |
|----------------------|
| New & Delete options |
| Start page options   |

|  |
|--|
| Users > Roles > <i>SelectRole</i> > Web > Bookmarks      |
| Users > Roles > <i>SelectRole</i> > General > UI Options |

Web > Java Socket ACL sub-tab

Resource Policies > Web > Java > Access Control > *SelectPolicy*

### 3.x User Interface Element

### 4.0 User Interface Element

Web > Cache Cleaner sub-tab

Enable/Disable

Users > Roles > *SelectRole* > General > Restrictions > Cache Cleaner  
AND Users > Authentication > *SelectRealm* > Authentication Policy > Cache Cleaner

Cleaner Frequency

Users > Authentication > *SelectRealm* > Authentication Policy > Cache Cleaner

Session Check Frequency

Users > Authentication > *SelectRealm* > Authentication Policy > Cache Cleaner

Files > General sub-tab

Enable Windows Networking

Resource Policies > Files > Windows > Access

Enable UNIX/NFS Networking

Resource Policies > Files > Unix/NFS

Files > Windows Access sub-tab

Resource Policies > Files > Windows > Access

Files > Windows Bookmarks sub-tab

Users > Roles > *SelectRole* > Files > Windows Bookmarks

Files > UNIX Access sub-tab

Resource Policies > Files > Unix/NFS

Files > UNIX Bookmarks sub-tab

Users > Roles > *SelectRole* > Files > UNIX Bookmarks

Email Client tab

Resource Policies > Email Client

Applications > General sub-tab

Enable Secure Terminal Access

Users > Roles > *SelectRole* > General > Overview

Enable Secure Application Manager options:

Enable using Windows version

Users > Roles > *SelectRole* > General > Overview

Enable using Windows version with Netbios

Users > Roles > *SelectRole* > SAM > Options

Enable using Java version and users can add applications

Users > Roles > *SelectRole* > SAM > Options

Enable using Java version

Users > Roles > *SelectRole* > General > Overview

Disabled

Users > Roles > *SelectRole* > General > Overview

Enable Automatic Launch of Secure Application Manager

Users > Roles > *SelectRole* > SAM > Options

Enable Automatic Uninstall of Secure Application Manager

*(not in beta)*

Applications > Terminal Sessions sub-tab

Resource Policies > Telnet/SSH

Applications > Secure Application Manager sub-tab (W-SAM)

Users > Roles > *SelectRole* > SAM > Applications

Applications > Secure Application Manager sub-tab (J-SAM)

Users > Roles > *SelectRole* > SAM > Applications

Applications > MS Exchange sub-tab (J-SAM)

Users > Roles > *SelectRole* > SAM > Add Application

Applications > Lotus Notes sub-tab (J-SAM)

Users > Roles > *SelectRole* > SAM > Add Application

Applications > Citrix NFuse sub-tab (J-SAM)

Users > Roles > *SelectRole* > SAM > Add Application

Meetings tab

Users > Roles > *SelectRole* > Meetings

| 3.x User Interface Element                                       | 4.0 User Interface Element                             |
|--|--|
| <b>Authentication &amp; Authorization &gt; Import Users menu</b> | Maintenance > Import/Export > Configuration            |
| <b>Authentication &amp; Authorization &gt; Active Users menu</b> | System > Status > Active Users                         |
| <b>Network Settings menus</b>                                    |  |
| <b>Network &gt; Network Settings menu</b>                        |  |
| Internal Port tab  | System > Network > Internal Port                       |
| External Port tab  | System > Network > External Port                       |
| Static Routes tab  | System > Network > Static Routes                       |
| Hosts tab  | System > Network > Hosts                               |
| Network Connect tab  | Resource Policies > Network Connect > IP Address Pools |
| <b>Network &gt; Clustering menu</b>                              |  |
| Status tab   | System > Clustering                                    |
| Properties tab   | System > Clustering                                    |
| <b>Network &gt; Web Proxy menu</b>                               |  |
| Web Proxy Server   | Resource Policies > Web > Web Proxy > Settings         |
| Unqualified Hostnames  | Resource Policies > Web > Web Proxy > Settings         |
| Exceptions   | Resource Policies > Web > Web Proxy > Policies         |
| <b>Network &gt; Email Settings menu</b>                          |  |
| <b>Network &gt; SNMP menu</b>                                    | System > Log Monitoring > SNMP                         |