

RANDY  
FRANKLIN  
SMITH'S


ULTIMATEWINDOWSSECURITY  
.COM

Preview of Key Points

- ❑ Domains and Forests
- ❑ Trust Relationships
  - Transitivity
  - Direction of trust
  - Risks of trust
  - External trusts
- ❑ Auditing trust relationships

© 2008 Monterey Technology Group Inc.

3

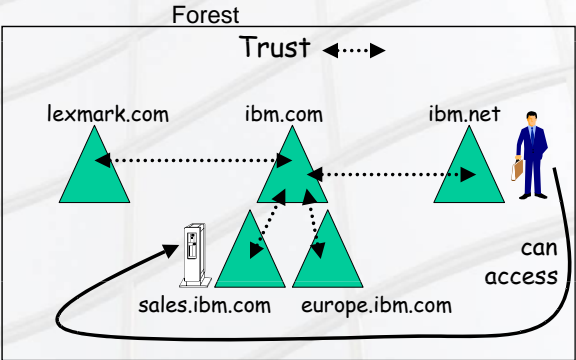


RANDY  
FRANKLIN  
SMITH'S

ULTIMATEWINDOWSSECURITY  
.COM

Domains and Forests

- ❑ The forest is the outer most, largest object in Active Directory
- ❑ A forest is essentially a set of domains that all trust each other.



The diagram illustrates a forest structure. At the top, the word 'Forest' is centered. Below it, a double-headed arrow labeled 'Trust' connects the domains. The domains shown are lexmark.com, ibm.com, and ibm.net, each represented by a green triangle. Below ibm.com are two sub-domains, sales.ibm.com and europe.ibm.com, also represented by green triangles. A dotted line connects lexmark.com to ibm.com, and another dotted line connects ibm.com to ibm.net. A solid line with an arrow points from a server icon to sales.ibm.com. A solid line with an arrow points from a person icon to ibm.net, with the text 'can access' next to it. A curved solid line with an arrow points from sales.ibm.com to europe.ibm.com.

© 2008 Monterey Technology Group Inc.

4

**AuditNet** & **RANDY FRANKLIN SMITH'S**  
The Global Resource for Auditors  
ULTIMATEWINDOWSSECURITY.COM

# Trust

- ❑ A trust relationship is a logical link between two domains facilitating transfer of authentication and authorization
- ❑ Users from the trusted domain can connect to servers in the trusting domain without reauthenticating or requiring a 2nd user account in the trusting domain

© 2008 Monterey Technology Group Inc. 5

**AuditNet** & **RANDY FRANKLIN SMITH'S**  
The Global Resource for Auditors  
ULTIMATEWINDOWSSECURITY.COM

# Trust

- ❑ Key trust terminology:
  - Trusting domain: Domain that allows access to users from another domain
  - Trusted domain: Domain that is trusted and whose users have access to the trusting domain

© 2008 Monterey Technology Group Inc. 6

**AuditNet** & **RANDY FRANKLIN SMITH'S**  
The Central Resource for Auditors  
ULTIMATEWINDOWSSECURITY.COM

# Trust

☐ Key trust terminology:

- One-way trust: One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain
- Two-way trust: Two domains allow access to users on each other's domain

The diagram shows two triangles representing domains. The left triangle is labeled 'marketing' and contains a 'resource' icon. The right triangle is labeled 'sales' and contains a 'User account' icon. A green arrow labeled 'trust' points from the marketing domain to the sales domain. A black arrow labeled 'Granted access' points from the sales domain back to the marketing domain. A second green arrow labeled 'trust' points from the sales domain back to the marketing domain.

© 2008 Monterey Technology Group Inc. 7

**AuditNet** & **RANDY FRANKLIN SMITH'S**  
The Central Resource for Auditors  
ULTIMATEWINDOWSSECURITY.COM


# Trust

☐ Key trust terminology:

- Transitive trust: Trust that can extend beyond two domains to other trusted domains in the tree
- Non-transitive (intransitive) trust: One way trust that does not extend beyond two domains

The diagram shows three triangles representing domains: accounting, marketing, and sales. In the top part, a green arrow labeled 'trust' points from accounting to marketing, and another green arrow labeled 'trust' points from marketing to sales. A black arrow labeled 'Trusts' points from accounting to sales. In the bottom part, the same setup is shown, but the black arrow from accounting to sales is crossed out with a red 'X' and labeled 'Trusts'.

© 2008 Monterey Technology Group Inc. 8



RANDY  
FRANKLIN  
SMITH'S


ULTIMATEWINDOWSSECURITY  
.COM

Trust Types

- ☐ Parent/Child
- ☐ Tree Root
- ☐ External
- ☐ Kerberos Realm
- ☐ Forest Trusts

© 2008 Monterey Technology Group Inc.

9

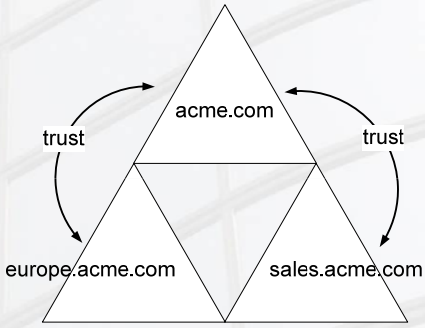


RANDY  
FRANKLIN  
SMITH'S

ULTIMATEWINDOWSSECURITY  
.COM

Trust Types


- ☐ Parent/Child
  - Trust between two AD domains that share a contiguous DNS namespace and belong to the same forest.



© 2008 Monterey Technology Group Inc.

10





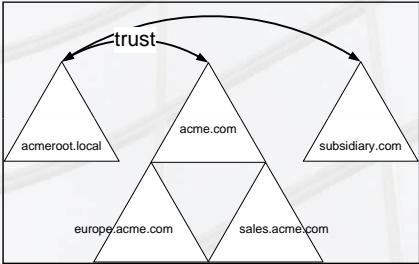
RANDY  
FRANKLIN  
SMITH'S

ULTIMATEWINDOWSSECURITY  
.COM

Trust Types


❑ Tree Root

- Trust between root domains in the same forest that do not share a common DNS namespace.



© 2008 Monterey Technology Group Inc.

11



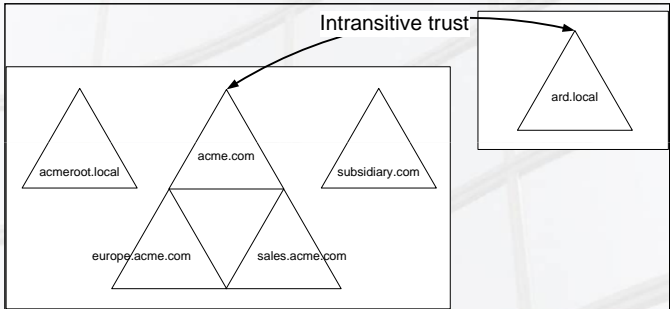
RANDY  
FRANKLIN  
SMITH'S

ULTIMATEWINDOWSSECURITY  
.COM

Trust Types


❑ External

- Trust used to connect to other domains outside of your forest; can also create a trust between an AD domain and NT4 domain or Samba domain



© 2008 Monterey Technology Group Inc.

12

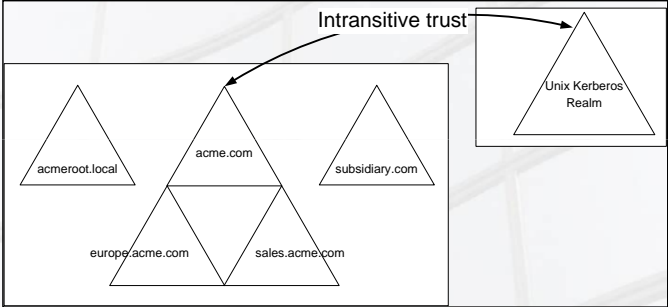


RANDY  
FRANKLIN  
SMITH'S  
ULTIMATEWINDOWSSECURITY  
.COM

Trust Types


☐ Kerberos Realm

- Trust between an AD domain and an MIT v5 Kerberos realm



© 2008 Monterey Technology Group Inc.

13

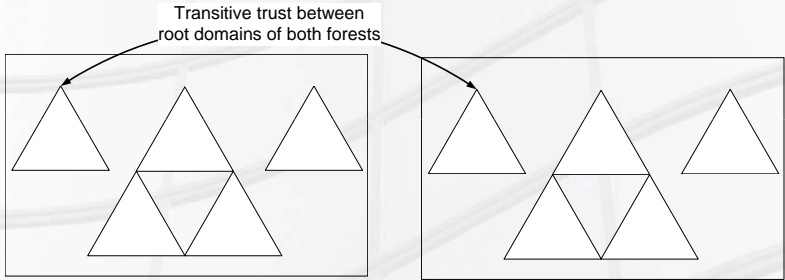


RANDY  
FRANKLIN  
SMITH'S  
ULTIMATEWINDOWSSECURITY  
.COM

Trust Types

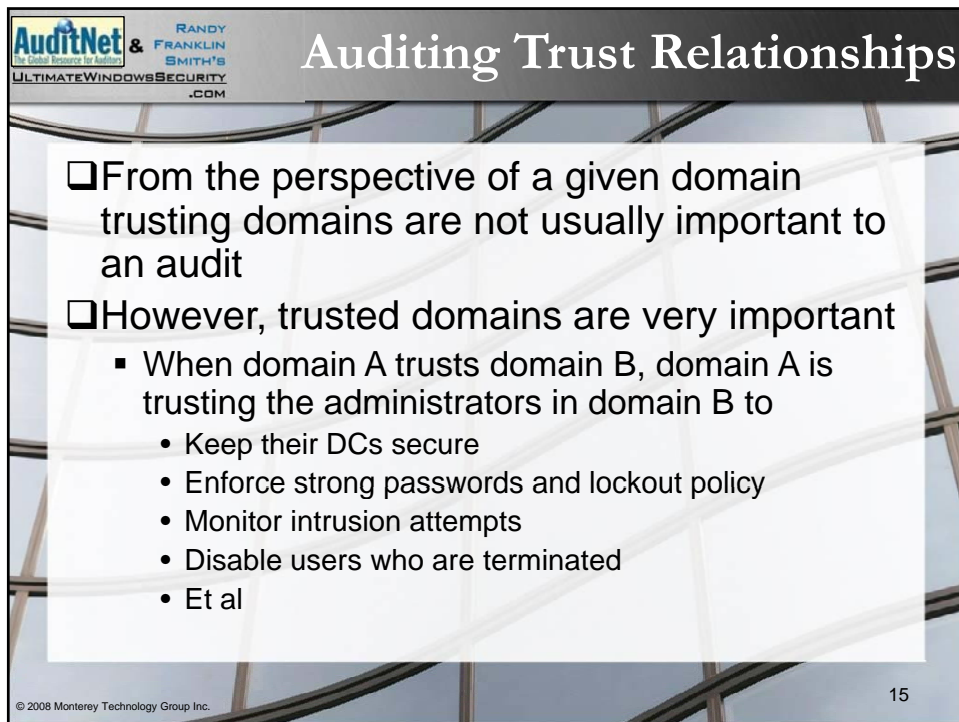
☐ Forest Trusts

- Trust between two AD forests
- Both forests must be running in Windows 2003 functionality level or higher



© 2008 Monterey Technology Group Inc.

14

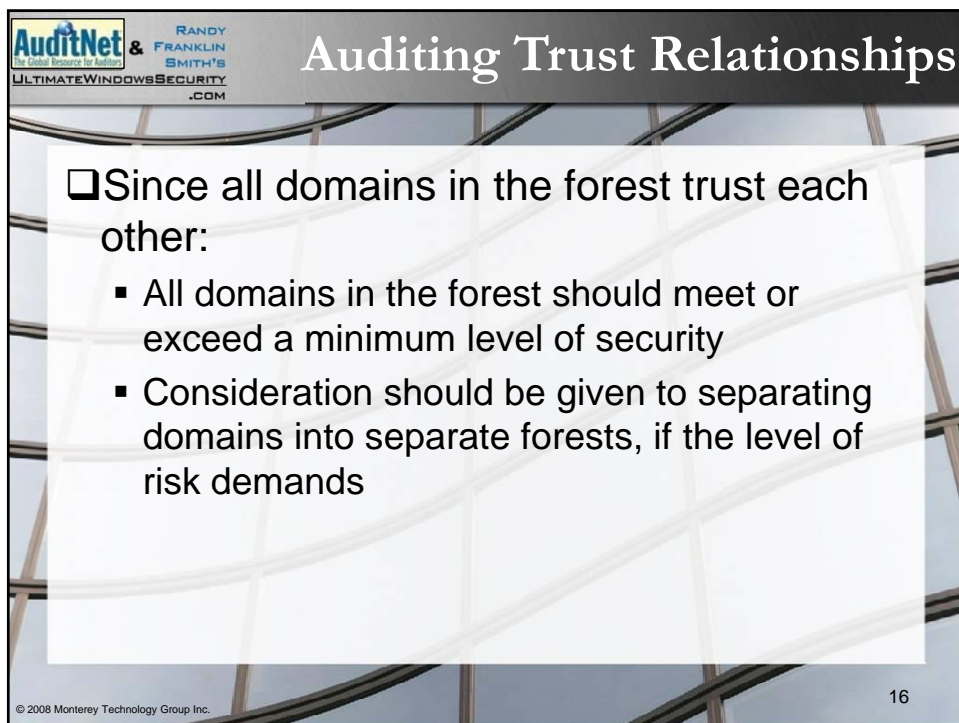


AuditNet & RANDY FRANKLIN SMITH'S  
The Central Resource for Auditors  
ULTIMATEWINDOWSSECURITY.COM

## Auditing Trust Relationships

- ❑ From the perspective of a given domain trusting domains are not usually important to an audit
- ❑ However, trusted domains are very important
  - When domain A trusts domain B, domain A is trusting the administrators in domain B to
    - Keep their DCs secure
    - Enforce strong passwords and lockout policy
    - Monitor intrusion attempts
    - Disable users who are terminated
    - Et al

© 2008 Monterey Technology Group Inc. 15




AuditNet & RANDY FRANKLIN SMITH'S  
The Central Resource for Auditors  
ULTIMATEWINDOWSSECURITY.COM

## Auditing Trust Relationships

- ❑ Since all domains in the forest trust each other:
  - All domains in the forest should meet or exceed a minimum level of security
  - Consideration should be given to separating domains into separate forests, if the level of risk demands

© 2008 Monterey Technology Group Inc. 16

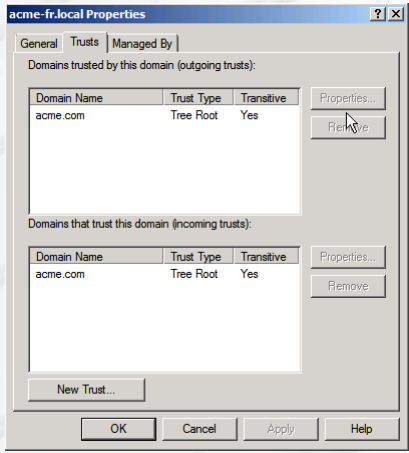




RANDY  
FRANKLIN  
SMITH'S  
ULTIMATEWINDOWSSECURITY  
.COM


## Auditing Trust Relationships

- ❑ Trust relationships can be viewed with Administrative Tools\Domains and Trusts
- ❑ Open properties for a given domain and examine its trusts



© 2008 Monterey Technology Group Inc.

17



RANDY  
FRANKLIN  
SMITH'S  
ULTIMATEWINDOWSSECURITY  
.COM

## Review Points

- ❑ All domains within the forest trust each other
  - No real separation between admins inside forest
- ❑ When assessing trusts ignore
  - Parent
  - Child
  - Tree root
- ❑ The only external trust that is transitive is a cross-forest trust
- ❑ External trusts that should be assessed
  - Realm
  - Forest
  - External
- ❑ Risk of a trust depends on
  - Difference in security quality between the 2 domains
  - Value of resources made available to trusted domain

© 2008 Monterey Technology Group Inc.

18




**AuditNet**  
The Global Resource for Auditors

**Where Savvy Auditors Go!**

Providing resources, tools, and information for auditors since 1993.

For more information go to <http://www.auditnet.org> or email [info@auditnet.org](mailto:info@auditnet.org)

Mention attendance at this Webinar and receive a free 30 day trial subscription to the AuditNet premium content



**AuditNet**  
The Global Resource for Auditors

**More help**

- ☐ Audit programs for Windows and AD
  - [www.ultimatewindowssecurity.com](http://www.ultimatewindowssecurity.com)

© 2008 Monterey Technology Group Inc.

The slide features a background image of a modern building with a glass facade. In the top left corner, there is a logo for 'AuditNet & FRANKLIN SMITH'S ULTIMATEWINDOWSSECURITY.COM'. The title 'More help' is positioned in the top right corner. The main content is organized into two columns, each with a square icon containing a checkmark. The left column lists 'Training by Randy Franklin Smith' and 'Consulting' services, while the right column provides 'Contact information' including an email address. A copyright notice is located at the bottom left of the slide.

**AuditNet & FRANKLIN SMITH'S**  
ULTIMATEWINDOWSSECURITY.COM

### More help

- ☐ Training by Randy Franklin Smith
  - On-site and on-demand
  - [www.ultimateWindowsSecurity.com](http://www.ultimateWindowsSecurity.com)
- ☐ Consulting
  - Outsourced and co-sourced audit services for Microsoft technologies
  - Remote and on-site
  - [www.montereytechgroup.com](http://www.montereytechgroup.com)
- ☐ Contact information
  - [rsmith@ultimateWindowsSecurity.com](mailto:rsmith@ultimateWindowsSecurity.com)

© 2008 Monterey Technology Group Inc.